3 SOFTWARE VULNERABILITIES AND THEIR CONSEQUENCES: COURSE OF EVENTS AND ANALYSIS

This chapter provides an answer to the first investigation question, namely how occurrences such as the security breaches caused by the vulnerability in Citrix software happened, what consequences they had and how those risks were managed. Section 3.1 describes what Citrix did after being informed of the vulnerability. Section 3.2 deals with the incident management and the consequences for the organizations using the software. To be able to extend the scope of the findings from the analysis of that occurrence, we then provide a description of other similar occurrences in section 3.3. To support the reader, the texts are provided with timelines.

3.1 Vulnerability in Citrix software and security breaches

This section describes the events that occurred following a vulnerability in Citrix software:[51] the discovery of the vulnerability, the response from the manufacturer and the incident management measures taken in the Netherlands from the moment that the manufacturer announced the vulnerability.

3.1.1 Discovery of vulnerability in Citrix software and response from the manufacturer

This subsection deals with the discovery of the vulnerability in the Citrix software and the response to the discovery by the manufacturer. The most important events are visualised in the following timeline.

51 Manufacturer Citrix published the vulnerability on 17 December 2019 (CVE-2019-19781).

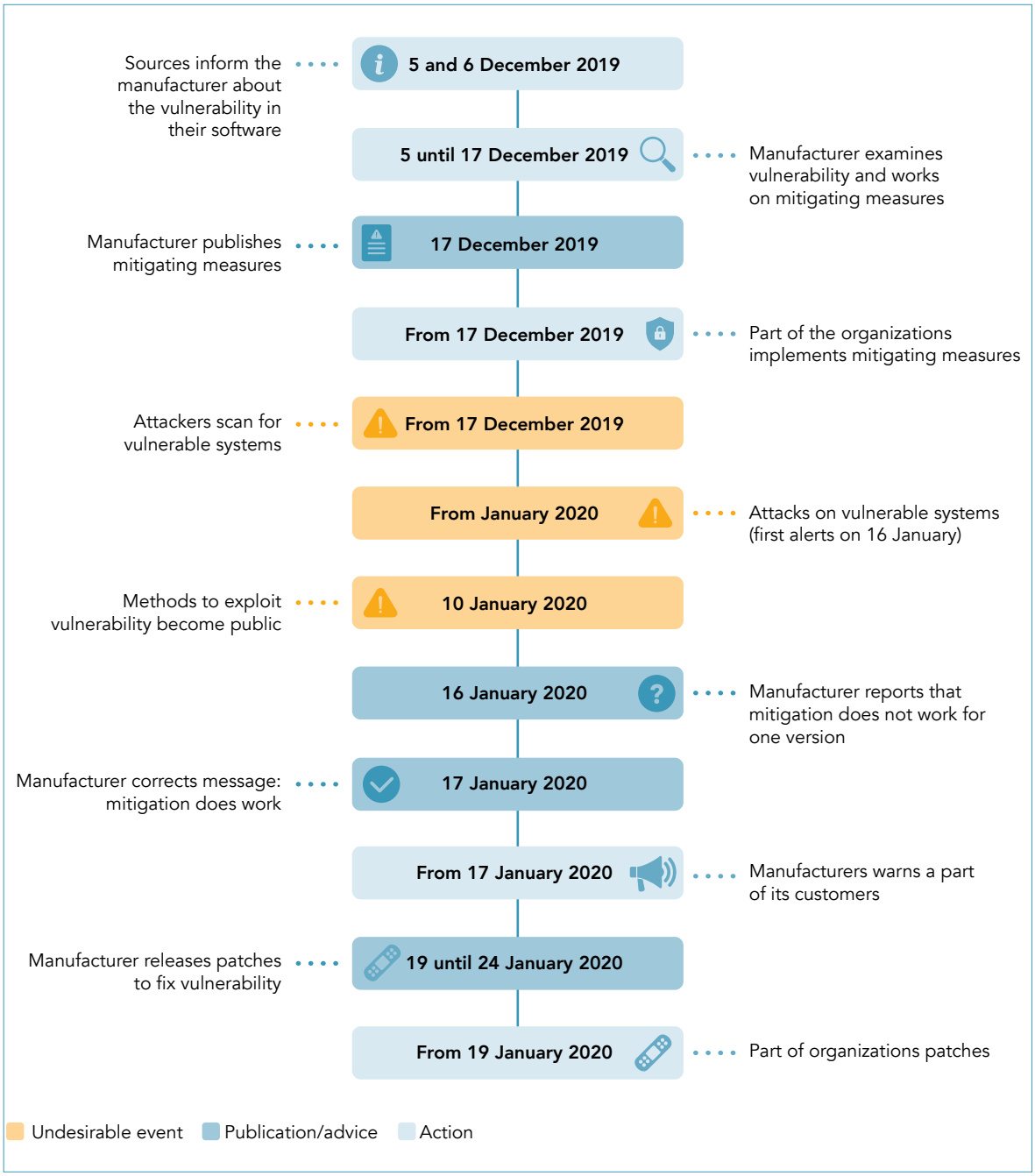

Figure 8: Timeline manufacturer.

Sources inform manufacturer about vulnerability in software

On 5 and 6 December 2019, three different sources approached Citrix. They informed the manufacturer independently of one another about the same vulnerability in the software. One of the sources indicated that the vulnerability was already more widely known. All three used the same method to demonstrate the vulnerability.[52]

52 Two of the sources indicated that they were not the original finder of the vulnerability, but that they had obtained the information from a bug bounty programme operated by one of Citrix's customers. According to this source, the vulnerability had been shared with other so-called bug bounty hunters, via online channels. Bug bounty hunters are individuals (or organizations) that in exchange for recognition or a reward go in search of vulnerabilities in digital systems. Interview CISO Citrix with Techzine, 23 January 2020. Available via: https://www.techzine.eu/blogs/security/44687/exclusive-interview-citrix-ciso-fermin-serna-where-did-it-go-wrong/

Manufacturer investigates vulnerability

Following these notices, Citrix investigated whether the vulnerability was known internally. This was not the case. A number of the manufacturer's departments then investigated the vulnerability. The manufacturer's analysis also revealed that this vulnerability had been present in the foundations of the software for more than ten years, in components that had been part of the product, since the start of its development.

Based on the fact that the PoC code would already be in circulation, the manufacturer estimated that vulnerable systems ran a high risk of being attacked. On the basis of this risk analysis, the manufacturer realized that this meant that the vulnerability was present in a large proportion of all versions (*installed base*) of the Citrix software in use, and that producing patches for all these versions would take a great deal of time and energy.

In response, and based upon the risk that a POC might be in circulation, Citrix decided to treat this as a zero-day vulnerability. The usual method is to first develop a patch aimed at repairing the vulnerability, and then publishing the vulnerability. Instead, the manufacturer developed mitigating measures as a temporary solution in advance of the definitive patches. A mitigating measure could be achieved faster than a patch. Even though a mitigating measure does not take away the cause of the vulnerability, it takes away the effect and reduces the risk. For this reason Citrix considered it to be as effective as a patch.

Manufacturer publishes mitigation steps

On 17 December, the manufacturer disclosed mitigating measures and the information on the vulnerabilities by publishing a support article and security bulletin on their website. In this bulletin, they warned of the vulnerability in various products and versions of the Citrix software. The manufacturer itself classified the vulnerability as very serious (9.8 on a scale of one to ten).[53]

Attackers scan for vulnerable systems

By publishing the mitigation steps, it became possible for attackers to derive where in the Citrix software the vulnerability was located and what type of vulnerability it was (*reverse engineering*) According to Citrix, the risk that a mitigation or patch might be reverse engineered to create an exploit, was outweighed by the importance of communicating the mitigation and the need to protect its customers from a zero-day situation.

In the week following the announcement, one of the sources that had reported the vulnerability published further details about the vulnerability. In the subsequent period, publications from other security researchers followed: based on the mitigation steps, they described the nature of the vulnerability, and how it could be abused to penetrate a vulnerable server. A worldwide scan on 8 January 2020 revealed that worldwide around 60,000 servers were using this product, and that of those around 40,000 still appeared to be vulnerable. For the time being, no one had published a working attack method, so

53 Citrix, *Support article Mitigation Steps for CVE-2019-19781*, created 16 December 2019, published 17 December 2019. Current version available via: https://support.citrix.com/article/CTX267679
Citrix, CVE-2019-19871 – *Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance*, 17 December 2019. Current version available via: https://support.citrix.com/article/CTX267027

it did not appear likely that at that moment attackers were in a position to exploit the vulnerability on a large scale, to attack vulnerable servers. Nonetheless, the manufacturer knew from the sources that had reported the vulnerability to it that the vulnerability and possibly the demonstration method were already circulating in particular groups.[54]

Methods for exploiting the vulnerability are made public

On 10 January 2020, via the platform GitHub and without consulting or notifying the manufacturer, a group of security researchers published the code for exploiting the vulnerability in the Citrix software. On 11 January, a security company also published its version of the exploit. Following the publication of the methods for exploiting the vulnerability, it became known both to the manufacturer and other stakeholders, such as the NCSC in the Netherlands, that an attack on vulnerable Citrix servers was very accessible even to non-expert attackers. The code was available on GitHub and on YouTube videos were published, demonstrating the method for exploiting the vulnerability. [55]

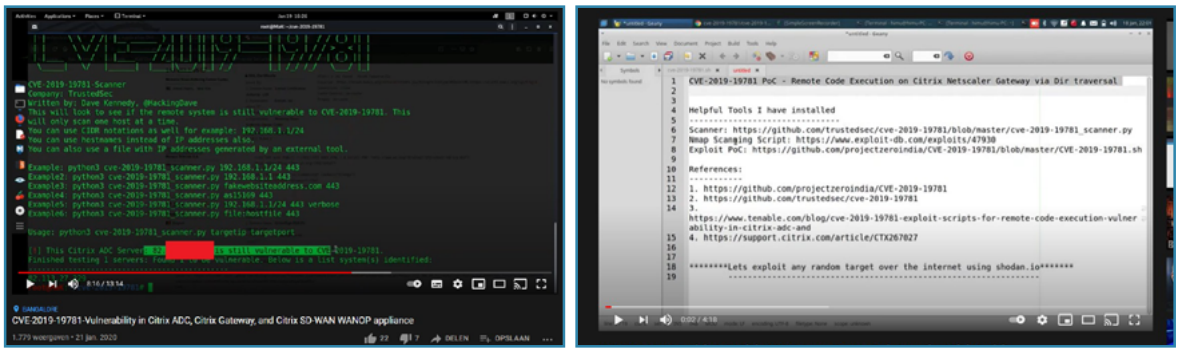

Figure 9: Videos (l) explaining how vulnerable servers can be found and (r) demonstrating how the vulnerability can be attacked.[56]

Vulnerable systems are attacked

In the days that followed, numerous reports were released about vulnerable and attacked servers. On 12 January 2020, for example, one security company published information about 25,000 vulnerable servers in the world, of which 713 in the Netherlands. The NCSC received a list of vulnerable servers from this security company on 11 January 2020. These were servers on which the organizations in question had not yet implemented the mitigation steps published by Citrix before they became under attack. This made the systems of which the servers were part of vulnerable to external attacks. Another security company issued a report on 15 January of a major spike in attacks. On that same day, a

54 Further details were published on: https://www.ptsecurity.com/ww-en/about/news/citrix-vulnerability-allows-criminals-to-hack-networks-of-80000-companies/ The term security investigator in this investigation refers to persons who on an individual basis or as part of a (security) company investigate vulnerabilities in software and systems. For example https://www.tripwire.com/state-of-security/vert/citrix-netscaler-cve-2019-19781-what-you-need-to-know/

55 GitHub is an online platform on which users can place source code, so that other users can make use of it.
Published exploit code 10 January 2020: https://github.com/projectzeroindia/CVE-2019-19781
Published exploit code 11 January 2020: https://github.com/trustedsec/cve-2019-19781

56 (l) https://www.youtube.com/watch?v=cALcgyq42kI (r) https://www.youtube.com/watch?v=c9-V68L5qUwI

hospital and a municipality announced that attackers had penetrated their systems making use of the vulnerability in the Citrix software.[57]

Mitigation received no priority

One government institution with limited IT capacity saw no possibility of implementing the mitigation steps for the Citrix systems, after it had been made available. The decision to not mitigate in this case was made by the IT department. This department was struggling with capacity problems and because they had already planned to replace the Citrix environment in the near future, they did not see immediate mitigation of the Citrix systems as a priority. The CISO[58] at this government institution was not able to communicate the urgency of the situation so that the IT department would implement the mitigation. As a consequence, the organization was attacked, and the Citrix systems had to be shut down. At this organization, this meant that employees could no longer work from home.

Doubts about the effectiveness of the mitigation steps

On 16 January 2020, one month following the publication of the mitigation measures, various sources reported that the mitigation steps as recommended by Citrix apparently were not effective for all versions of the Citrix ADC and Gateway. The manufacturer published a notice stating that for certain older versions of the software, the mitigation was not fully effective, but soon afterwards realized that this conclusion had been drawn erroneously. On 17 January 2020, Citrix corrected the published notice via a bulletin update and executives of the manufacturer reported explicitly in a TV interview, blogpost and on Twitter that the mitigation steps were effective for all releases and patches, on condition the customer had implemented all steps necessary for ensuring the correct functioning of the mitigation. The alternative was to upgrade to a new version, and to implement partial migration.[59]

Manufacturer warns group of customers

One day earlier, on 15 January 2020, Citrix took additional measures beyond the previously published mitigation measures, as an interim solution until the patch for the vulnerability became available. The manufacturer launched a tool on 15 January to test whether machines were vulnerable and whether the mitigation was correctly executed. The NCSC requested Citrix on 17 January to also develop a forensic tool to determine whether a vulnerable server was accessed. As such tool was not yet available, Citrix built it pursuant to the NCSC request and made it available on 22 January.

57 Publication 12 January 2020:
https://badpackets.net/over-25000-citrix-netscaler-endpoints-vulnerable-to-cve-2019-19781/
https://www.security.nl/posting/639015/Honderden+Nederlandse+Citrix-servers+kwetsbaar+voor+aanvallen.
https://www.fireeye.com/blog/threat-research/2020/01/vigilante-deploying-mitigation-for-citrix-netscaler-vulnerability-while-maintaining-backdoor.html
https://nos.nl/nieuwsuur/artikel/2318812-hack-poging-in-ziekenhuis-en-gemeente-urgentie-lek-leek-niet-duidelijk.html and https://www.ad.nl/tech/ziekenhuis-leeuwarden-legt-dataverkeer-met-buitenwereld-stil-na-cyberaanval~a45daf1e/

58 Chief Information Security Officer responsible for information security within an organization.

59 Depending on the license and support contract, there could be a cost to the customer for the upgrade.
Notice that mitigation for one version didn't work https://support.citrix.com/article/CTX269189
Correction of previous notice: https://www.citrix.com/blogs/2020/01/17/citrix-updates-on-citrix-adc-citrix-gateway-vulnerability/

In addition to placing the alert on the website and in social media reports, the manufacturer attempted to reach as many of its customers as possible. In the period between 17 and 24 January, Citrix sent out more than 124,000 emails to approximately 36,000 different organizations. During this same period, the manufacturer started to establish a database with contact details for its customers[60], so that in the event of future vulnerabilities it would be possible to trace products and warn customers more effectively.

From the start of January 2020, the manufacturer (and others like the security researchers of DIVD, see section 3.1.2) also started to scan the internet for IP addresses of vulnerable servers.[61] If the manufacturer was able to link a located IP address to a customer, they attempted to actively approach the customer in question. In consultation with the NCSC, Citrix also shared the IP addresses it had identified in this way, with the national CERTs, including the Dutch NCSC.

Manufacturer publishes patches to definitively repair the vulnerability

On 17 January, Citrix published a timeline showing when the patches that would definitively repair the vulnerability were due to be published. Citrix initially expected that it would need until 31 January to produce patches for all versions of the various products in circulation. Citrix eventually published the patches in the period 19 to 24 January.[62]

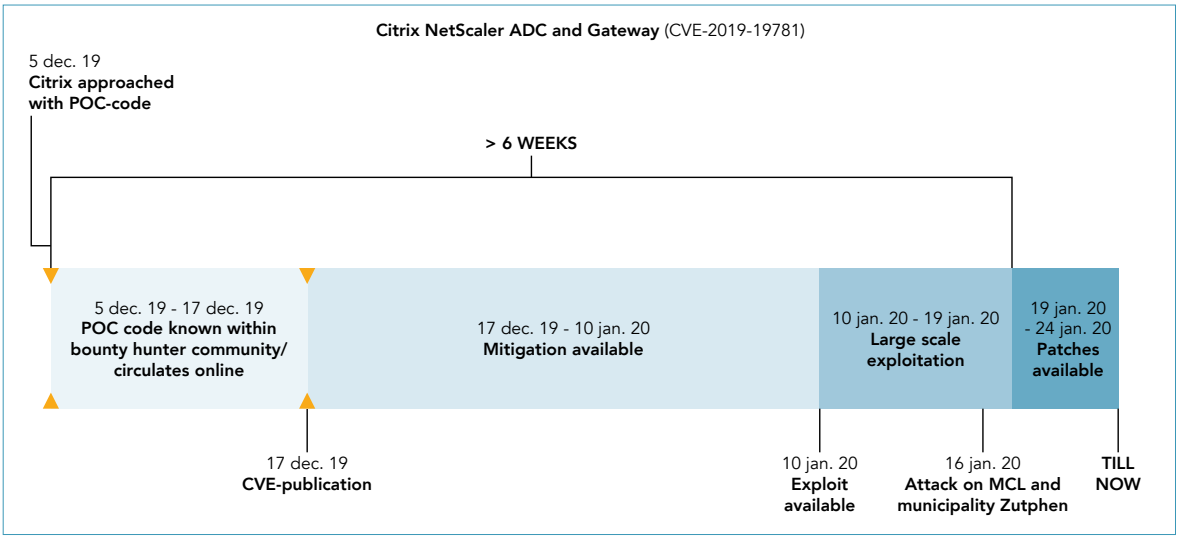

Figure 10: Timeline from discovery of vulnerability through to publication, operation and patches.

60 Customer Relationship Management (CRM).

61 In that process, Citrix made use of a tool produced in-house, in combination with such services as BinaryEdge and Shodan. These services scan the internet to classify devices linked to the Internet (approachable from a specific IP address and gateway combination).

62 A patch is a new version of the software that no longer contains the vulnerability (source: *Woordenboek Cyberveilig Nederland 2019*). First timeline of patches: https://www.citrix.com/blogs/2020/01/11/citrix-provides-update-on-citrix-adc-citrix-gateway-vulnerability/ Publication of patches: https://www.citrix.com/blogs/2020/01/22/update-on-cve-2019-19781-fixes-now-available-for-citrix-sd-wan-wanop/

3.1.2 Consequences and incident management in the Netherlands

This subsection deals with incident management in the Netherlands from the moment that the manufacturer announced the vulnerability.

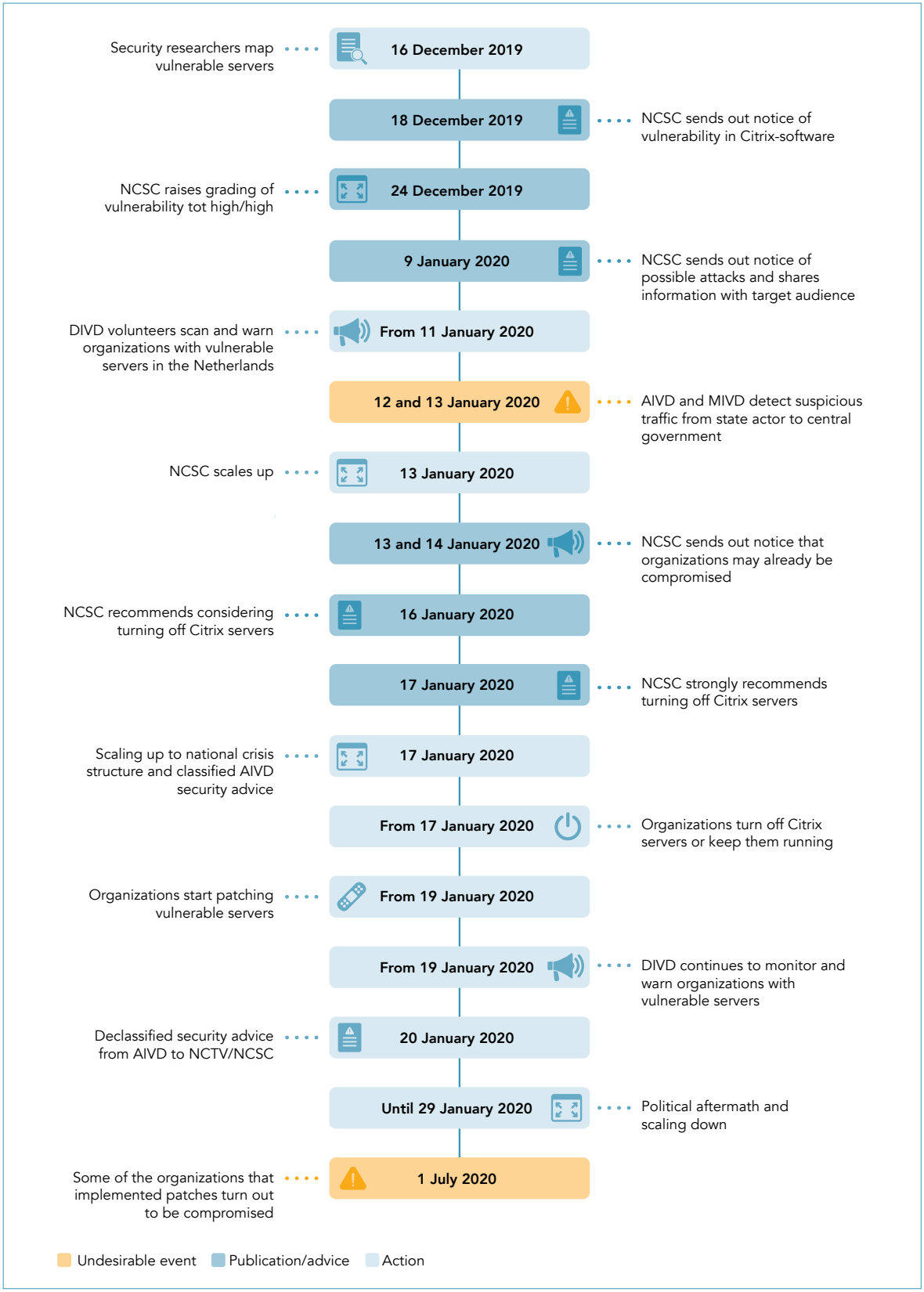

Figure 11: Timeline incident response[63].

63 It is not possible anymore to determine whether these organizations had mitigated in advance, and whether this was done correctly and timely.

Security researcher scan the internet for vulnerable servers

Various security researchers including from DIVD[64] scanned the internet to map out how many servers were using the vulnerable Citrix software. A first scan on 16 December 2019 revealed more than 125,000 vulnerable servers worldwide; on 23 December (one week after publication of the vulnerability), there were still 80,000 vulnerable servers, of which 3,700 in the Netherlands. On 7/8 January 2020, there were still 700 vulnerable servers in the Netherlands.

NCSC warns of vulnerability in Citrix software

On 18 December, the Dutch NCSC published an initial security recommendation about this vulnerability on its website. It also shared the recommendation with its own target groups: national government and vital operators: 'NCSC security recommendation 18 December 2019: Citrix reports that a vulnerability has been discovered in Citrix ADC, Citrix Gateway, Citrix NetScaler and Citrix NetScaler ADC. The vulnerability has also been found in the Citrix SD-WAN WANOP software.' The NCSC identified the seriousness of the vulnerability as medium/high. Based on further information from security investigators, on 24 December, NCSC raised the grading of its earlier security recommendation to high/high and informed its target organization about this.[65]

NCSC warns of possible attacks and shares information with target groups

On 9 January, the NCSC warned its target organizations, and published a bulletin on its website that attackers were actively seeking out vulnerable Citrix servers. This warning was based on notices issued among others by the Internet Storm Center of SANS. The Fusion Center[66] of the NCSC received multiple signals from their target groups that they could observe attackers were seeking out vulnerable severs. The Fusion Center also received lists of IP addresses from security investigators listing more than 700 vulnerable servers. They included this information in an update of their security advice on the website.[67] After the NCSC's security advisory was raised to High/High, the DTC informed the non-vital target group about the vulnerability on several occasions and offered them action perspective.

On 10 January 2020, the Fusion Center again informed various target group organizations by telephone. In the days following NCSC alsoshared information with the affiliated sectoral CERTs[68]. On grounds of societal interest, the director of the NCSC granted permission to also share data they consider to be personal data and/or confidential

64 The Dutch Institute for Vulnerability Disclosure (DIVD) is a Dutch organization consisting of security investigators who voluntarily offer their services, in their own words 'to make the digital world a safer place by tracing and reporting vulnerabilities to the people who can solve the problem'.
Report DIVD: https://www.divd.nl/reports/2020-00001-Citrix/
Message on vulnerable Citrix servers: https://www.ptsecurity.com/ww-en/about/news/citrix-vulnerability-allows-criminals-to-hack-networks-of- 80000-companies/

65 Notice from NCSC: https://www.ncsc.nl/actueel/advisory?id=NCSC-2019-0979 update 18 December 2019.
Grading matrix of the NCSC:
medium/high: average risk of abuse and high impact in the event of abuse.
High/high: high risk of abuse and high impact in the event of abuse.

66 Operational core of the NCSC where (inter)national information flows are processed 24/7.

67 Message from the Internet Storm Center of SANS: https://isc.sans.edu/forums/diary/A+Quick+Update+on+Scanning+for+CVE201919781+Citrix+ADC+Gateway+Vulnerability/25686/ 7 January 2020.
Among others the Water-ISAC and IWWN network.
https://www.ncsc.nl/actueel/advisory?id=NCSC-2019-0979 update 9 January 2020.

68 IBD, SurfCert, Cert WM, ZCert. For example, SurfCERT indicated that it was briefed by NCSC in the evening of January 13.

traceable information.[69] This permission was necessary according to NCSC because it finds it has no legal authority to share this information with these organizations. Section 4.3 addresses these considerations. The NCSC also requested the CIO Rijk to inform the CIOs, CTOs and CISOs of the various government departments. The CIO Rijk asked the departments whether they had taken the necessary measures, and asked them to do so if necessary. According to the NCSC, at that time organizations that had not yet applied the mitigation steps to their Citrix systems should assume that their systems had been compromised.

NCSC scales up

On 11 January, the NCSC noticed that exploit codes had been published on 10 January. Those exploit codes could be used to exploit vulnerable systems. In response, the NCSC once again updated its security advice for its target organizations and the general public. In response to signals that large numbers of vulnerable servers in the Netherlands could be penetrated, NCSC deployed its event team on 13 January.[70]

At that time, the event team assessed that the Citrix software was in use by a great number of Dutch organizations, but there was no complete picture of which Citrix users were still vulnerable. Within the NCSC there were doubts about the effectiveness of the mitigating steps published by the manufacturer Citrix. In addition, various organizations had not yet implemented these mitigation steps. The event team focused on informing as many organizations as possible on the vulnerabilities.

AIVD and MIVD recognize suspicious traffic

The intelligence services were able to determine that offensive activities were being carried out by a state actor because, through the deployment of special resources, they have insight into the digital infrastructure used by this state actor and can relate this to digital traffic to the national government. This suspicious digital traffic was recognized on January 12 and 13, immediately investigated further, explained and reported on to various policy departments in the intelligence report mentioned above.

DIVD scans and warns organizations with vulnerable servers in the Netherlands

On 11 January, the DIVD deployed a Security Hotline (currently named DIVD CSIRT). From this Hotline, they initially approached organizations with vulnerable Citrix servers themselves by sending an automatic email with a warning and recommendations to the suspected mail addresses of the organizations related to the vulnerable IP addresses. The DIVD (currently named DIVD-CSIRT) also passed on the list of vulnerable IP addresses

69 The NCSC is an implementing organization with respect to the tasks of the Minister of JenV regulated in the Wbni and operates within the established policy and legal frameworks. These frameworks indicate that personal data or information that can be traced back to it can only be shared with organizations that have been designated as OKTT or CERT.

70 Update security advice: https://www.ncsc.nl/actueel/advisory?id=NCSC-2019-0979 update 11 January 2020. The NCSC operates various upscaling or escalation levels. In principle, incidents are dealt with by incident handlers who tackle minor problems at organizations. If incidents become too large to be able to be implemented within the regular tasks, upscaling takes place. The first step is the event team, a specific team that is deployed during office hours to relieve the regular operation. If the situation becomes more urgent, or if the problem is larger, the next level of upscaling is the disaster team, whereby it is also possible to continue working outside office hours. In 2020, the NCSC scaled up on two occasions to the highest level: during the Citrix occurrence and during the SolarWinds occurrence. It is possible to further upscale to crisis level, at which point the NCTV takes over coordination.

to internet providers (network owners), in particular KPN and NBIP (National Internet Providers Management Organization) and to sectoral CERTs such as the CERT for the healthcare sector (Z-CERT) and NCSC.[71] Following the scans of the DIVD and other parties, the CSIRT-DSP immediately notified the compressed parties from its own target group (digital service providers).

NCSC publishes notice to organizations that they could already be compromised
On 13 January, the NCSC once again sent a bulletin to its target groups, and on 14 January they published a notice on their website.[72] In that bulletin the NCSC advised urgently to mitigate the vulnerability as soon as possible, as recommended by Citrix. Even if these mitigation measures had recently been taken, the NCSC once again warned of the possibility that attackers may already have access to their systems. From various organizations, the NCSC received requests for more information following this notice.

Dutch organizations report being compromised
On 14 January, the CERT for the municipalities, IBD, informed the NCSC that a municipality had reported abuse of its system. The Citrix servers had been attacked, and the decision had been taken to shut down the systems. On 15 January, the NCSC received a report from a hospital that it too had been attacked, and that it had consequently shut down all data traffic with the outside world. Employees were unable to work from home, and patients were no longer able to access their patient file. The vulnerability in Citrix software received much media attention. External experts reported to the NCSC that organizations were definitely compromised, if they had not taken measures before 9 January. More reports were received from organizations where attackers had penetrated their systems: the rail sector, the police central control room, municipalities and a hospital. The NCSC received a list of vulnerable IP addresses from Citrix, and shifted its focus to advising and informing the target groups. The media attention grew, and with it the pressure on NCSC, for example with the growing number of questions for the NCSC from organizations that use Citrix software.

NCSC publishes Security Advice: consider shutting down Citrix servers
As described in 3.1.1, on 16 January, manufacturer Citrix issued a notice that said the mitigating steps were not effective for one version of the software. One day later, the manufacturer corrected this report in the form of a bulletin update.

On 16 January, the NCSC published a security advice in which it recommended to to consider shutting down the Citrix servers, depending on the impact this would have on the organization involved.[73] This advice was in part provoked by the uncertainty on the effectiveness of the mitigation steps caused by Citrix' erroneous message, and the assumption that many organizations had not yet or not yet fully implemented the mitigating measures. On the basis of NCSC' security advice, the Dutch House of

71 Using an automated script that sent mails to info@, abuse@ and security@ mail addresses belonging to the relevant IP address and the connected domain.
NBIP was established by Internet service providers as a collective means of dealing with tap requests. Since that time, they have also developed a system for countering DDoS attacks. https://www.nbip.nl/en/about-the-nbip

72 Notice from NCSC: https://www.ncsc.nl/actueel/nieuws/2020/januari/13/vele-nederlandse-citrix-servers-kwetsbaar-voor-aanvallen

73 This notice is no longer available on the NCSC website. The title is 'mitigating measures recommended by Citrix not always effective', and was sent on 16 January 2020. The notice appears in Appendix C.

Representatives, Amsterdam Airport Schiphol, various Ministries, Municipalities, other (government) organizations and private companies shut down their Citrix systems. The NCSC received numerous questions both from target group organizations and organizations outside its target group, seeking further information as a result of the NCSC security advice. There was considerable unrest among these organizations about the reliability of the mitigating measures recommended by Citrix.

Deploying the national crisis structure and AIVD security advice
Given the seriousness of the situation, the National Crisis Centre (NCC) decided to partially deploy the national crisis structure, by summoning the IAO (Interdepartmental Coordination Consultation). The NCTV coordinated this interdepartmental coordination. Within the NCSC, the team scaled up to the level 'emergency' and assembled the emergency team.

On 17 January, the MIVD and AIVD issued an information notice to the NCTV and NCSC stating that it had identified an acute state actor threat aimed at an organization within national government. The Cabinet mandated the Minister of the Interior and Kingdom Relations and the Minister of Justice and Security to deal with the crisis.

In the afternoon, it became clear that there was a difference of understanding between the AIVD and the NCSC concerning the Security Advice to be issued to national government. This resulted in two different Safety Advices being laid on the table: the AIVD wanted NCSC to strongly advise organizations to shut down all Citrix servers, because, according to them, the patch did not fully work for all versions of the Citrix software, while the NCSC wanted to advise organizations to reach their own decision to shut down based on their own specific situation.

NCSC publishes urgent Security Advice: shut down Citrix servers
On the basis of the two different security advices, the Minister of Justice and Security, the Minister of the Interior and Kingdom Relations, in consultation with the NCTV, decided on 17 January that NCSC should aggravate their security advice from the NCSC and line up with the AIVD security advice. The NCSC was ordered to issue an urgent security advice to national government and the vital operators to shut down Citrix servers, based on uncertainty about the effectiveness of the mitigation steps recommended by Citrix, and the recognized threat. Starting point of NCSC's advice was the 'comply or explain' principle. CIO Rijk applied this principle in the national government. The security advice remained valid until an effective solution was available. NCSC broadcast the security advice via a target group notice, a press release on rijksoverheid.nl, the NCSC website and via other cybersecurity organizations in the Netherlands.

Each individual organization was required to make its own assessment of the impact and bore primary responsibility for its own measures and its own 'explanation if it chose to not shut down its Citrix servers. National government parties were required to present their 'explanation' to CIO Rijk, for assessment. With regard to the vital operators, the NCSC was able to offer advice and assistance where possible. The NCSC was also in consultation with Citrix on the situation. If the parties opted for 'comply', the impact of

shutting down Citrix servers on the work varied between organizations. In many cases, homeworking was no longer possible, which would lead to a rise in the number of employees travelling to the offices, which in turn would lead to increased traffic congestion during peak hours, while for other organizations, shutting would have more drastic consequences.

The urgent security advice from the NCSC was based on the security advice from the AIVD. The underlying intelligence notice contained information that was classified as state secret, and therefore not allowed to be published. The security advice itself was not classified. The NCSC did not communicate with other organizations about the content of the security advice, because of the classification of the information. Among organizations that received the NCSC security advice, there was confusion about the nature of the advice of 17 January, because it differed from the previous advice issued by the NCSC on 16 January, in particular the less urgent advice to consider shutting down Citrix servers. The recommendation from the NCSC was also more urgent than the advice from Citrix itself, from security companies advising the organizations, such as Fox-IT, and from national CERTs and security companies in other countries. Organizations indicated that they were unable to determine whether the more urgent advice also applied to them, and whether they needed to take action in response. NCSC could not initially share the content of AIVD's security advisory with the organizations outside the national government because of its classification. AIVD declassified the message on January 20. This did not give rise to NCSC to share the security advice at that moment.

Organizations decide whether or not to shut down Citrix servers

Shutting down the Citrix servers had different consequences for different organizations. For certain organizations, such as government departments, the consequences were limited to not being able to work at home.[74] At a number of municipalities, shutting down the Citrix servers meant it was no longer possible to pay social security supplementary benefits to residents of the municipality. The Ministry of Economic Affairs and Climate Policy chose to leave its Citrix servers switched on, because they were convinced they applied the mitigating steps in time, and because shutting down would have meant that the Netherlands Food and Consumer Product Safety Authority (NVWA) would have been unable to carry out any further inspections and customs checks. Without these checks the meat production and trade would have to be halted. In hospitals, patients were no longer able to access their electronic patient file, and in certain cases communication with other hospitals became impossible. There were also organizations that experienced little to no negative impact from the occurrence: their Citrix servers played a minor role in their digital system or they had access to an alternative.

74 It should be noted in this respect that the occurrence took place several months before most employees were required to work from home due to the COVID-19 pandemic, starting in March 2020. The consequences of such an occurrence in that period would have been far more far-reaching than they were in January 2020.

Dependency on Citrix software greater than assessed
Many businesses and Ministries use Citrix servers for the operation of their internal applications, or work with service providers and suppliers who use Citrix software. In many organizations Citrix servers function as a hub for a whole range of applications deep within the organizations' IT. Citrix software is above all known for working from home. However, it is also used as a point of access for example for email and office applications or for primary processes.

One of the government organizations performed a risk analysis to decide whether the systems should be shut down. After shutting down it became clear that more processes were dependent on Citrix software than previously estimated: in their risk analyses they had only identified between 60 and 70 percent of its dependencies on Citrix software. After shutting the Citrix-servers down, the dependency turned out to be so extensive that eventually not a single digital operating process could be continued.

From 9 January onwards, the CIO Rijk had called the CIOs, CISOs and CTOs of national government to follow the security advice of the NCSC, and had asked them to notify the CIO Rijk of the status of their compliance: had the organization shut down its Citrix servers, and if not, what was their reasoning.

Following the security advice of 17 January, CIO Rijk started drawing up a situation report on the compliance of government organizations, for the IAO. The majority of national government organizations (61%) that had responded had shut down their Citrix servers; a small proportion (20%) had left the Citrix servers switched on, reasoning that it would be a threat to national security to switch them off, that their department was protected by multilayer security, or because shutting down could result in too great an impact on critical processes or could cause social or economic damage. 19% of the organizations within national government did not use Citrix software at all. The Minister of Justice and Security and the Minster of the Interior and Kingdom Relations reached out to sectoral CERTs to obtain a clear picture of the extent to which their target organizations had complied with the recommendation from the NCSC to shut down the Citrix servers.

Situation sketch Citrix servers in government
Almost all the target group organizations of the NCSC, such as national government and the House of Representatives used Citrix:
- of the 12 Ministries, 10 used Citrix software;
- of the 69 national government organizations, 56 used Citrix software; of those, 42 shut down parts of the system.

Other public authorities:
- 150-200 of the 352 municipalities used Citrix software, and 80% of them shut the system down;
- 9 of the 12 provinces used and shut down Citrix software;
- all 22 water authorities used Citrix software. The majority shut down Citrix servers; a number remained operational for compelling reasons;
- 16 of the 25 security regions used Citrix software.

Organizations start patching vulnerable servers

After spending the weekend conducting continuous activities around Citrix, the disaster team of the NCSC gathered again on 18 January 2020 and noted the growing media attention.

On 19 January, Citrix released the first patches and the NCSC advised the organizations to urgently implement these. These patches were only suitable for a proportion of the versions of the Citrix software; around 50% of the vulnerable Citrix systems in the Netherlands. NCSC maintained its advice: shut down Citrix servers or explain why not (comply or explain). In addition, the NCSC issued advice on the announced patches and how to re-establish safe working environments. The NCSC indicated that organizations should assume that they had been compromised, if they had not taken the appropriate mitigation steps on time (see subsection 3.1.1: on time meant before the method for exploiting the system became public knowledge). See also the flowchart below, that NCSC published on 20 January so organizations could carry out their own risk analysis with regard to the Citrix vulnerability.

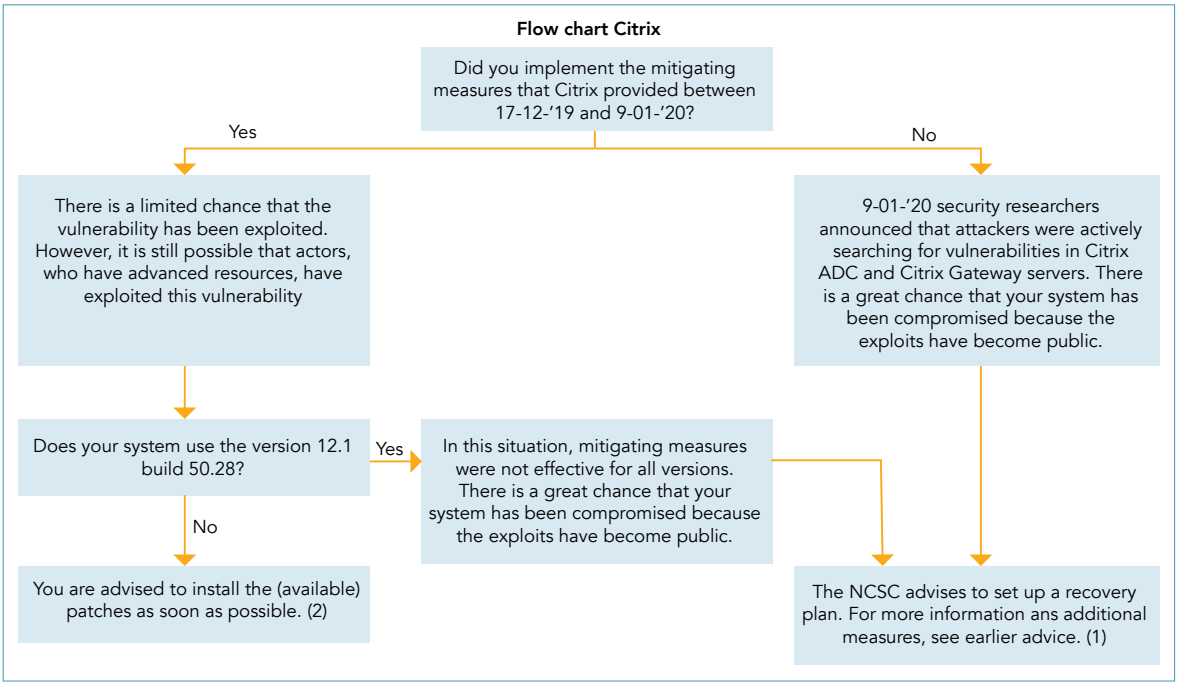

Figure 12: Flowchart Citrix. (Source: NCSC)[75]

A mail was then sent to all national government organizations with work instructions, addressed to civil servants with regard to the impact and potential for response. Within the NCSC, there was discussion as to whether they could scan for vulnerable servers themselves. Given the technical risks and legal restrictions, the NCSC decided not to do this (section 4.3 addresses these restrictions). This decision was also influenced by the presumption in the cybersecurity strategy that organizations themselves are responsible for monitoring their Citrix environment and the underlying systems. When on 21 January a number of organizations using Citrix software reported to the NCSC that they had identified malware on their systems and requested support for a forensic investigation,

75 https://www.ncsc.nl/documenten/publicaties/2020/januari/20/stroomschema-risicoafweging-citrix

the NCSC decided that it should restrict itself to its statutory task due to capacity considerations, and would not provide the requested support. Organizations should turn to security companies with forensic expertise. However, all of those companies were fully occupied at the time, assisting their existing customers: some organizations could not immediately receive the support they needed.

In collaboration with a number of operational partners, the NCSC also started testing the patches provided by Citrix, and the previously recommended mitigation measures. On 24 January, the NCSC sent a notice to all its target organizations that it had verified that the new patches were effective. In the target group notice and on the website, the NCSC issued recommendation security advice to have a forensic investigation carried out. National government organizations were obliged to report to CIO Rijk and the NCSC if the organization decided to switch on its Citrix servers again.

DIVD continues to monitor and issue warnings

On 15 January, the Security Hotline of the DIVD had also issued a advice to organizations within The Netherlands on how to check whether a system in which the mitigation measures had been implemented after 11 January had already been taken over. Depending on the seriousness of the attack organizations should determine whether or not it was necessary for them to carry out a forensic investigation or even to opt to fully reinstall the system. In the months following the release of the patches, the DIVD continued to scan the non-mitigated (vulnerable) servers. The number of vulnerable servers started to fall. On 3 February 2020, 70 vulnerable servers remained; by the start of March 2020 only five. New DIVD volunteers called these organizations once again and reissued the warning to the relevant managers, or left requests along the same lines with the receptionist.[76]

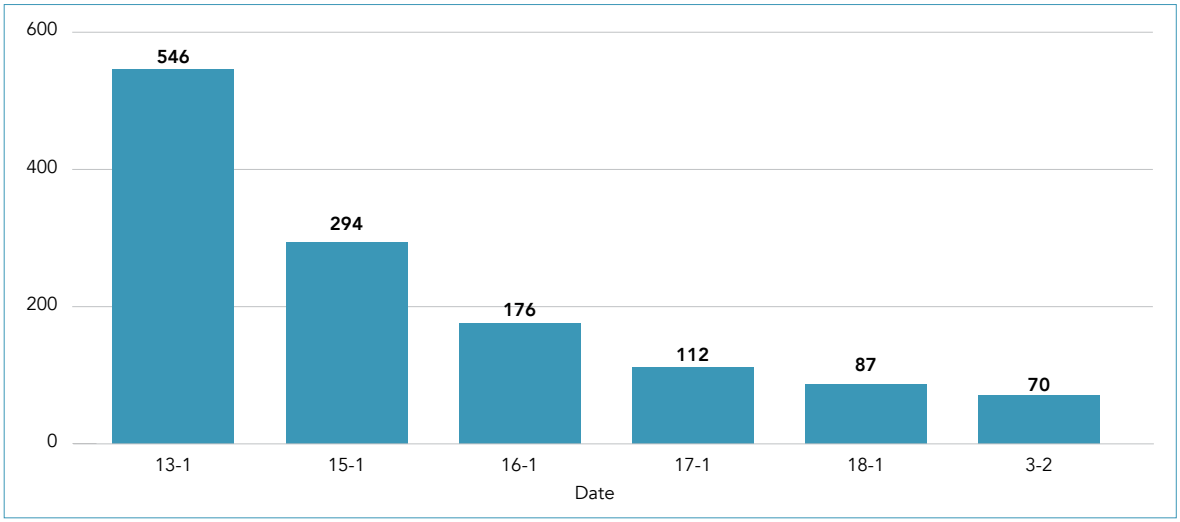

Figure 13: Non-mitigated Citrix systems found by DIVD CSIRT. (Source: divd.nl)

76 Advice from Security Hotline of the DIVD: https://csirt.divd.nl/2020/01/15/How-to-check-your-Citrix-gateway/ In practice, it appeared that these organizations were not yet aware of the DIVD Security Hotline. As a result, the security researchers were not always passed on to the relevant IT manager.

Terminating crisis structures and political aftermath
On 20 January, the Interdepartmental Crisis Management Committee (ICCb) met. The problems surrounding Citrix were discussed in the ICCb. By means of a Letter to Parliament entitled 'Vulnerability in Citrix products', the Minister Justice and Security and the Minister of the Interior and Kingdom Relations informed the Dutch House of Representatives on the identified vulnerability in Citrix products, the warning and the security advice from the NCSC.

In response to the Question Time in the House of Representatives on 21 January, on 23 January, the Minister of Justice and Security sent a report of the facts relating to the vulnerability in Citrix software to the Dutch House of Representatives, and provided a technical briefing. On 24 January, via a ministerial decree, the Minister of Justice and Security identified four sectoral CERTs[77] with whom the NCSC was allowed to exchange information more intensively.

On 29 January, the seventh and final Interdepartmental Coordination Consultation session was held. From that moment onwards the crisis structure was terminated: the activities regarding the vulnerability in the Citrix software were undertaken via the regular reporting lines, both within the NCSC and the whole of national government.
On 31 January 2020, the majority of departments had switched all their systems back on. A number of government organizations required a recovery plan before they could return to their normal working situation. The NCSC and the CIO Rijk did form a task group, that took further control of winding up the activities relating to the vulnerability in the Citrix software.

Some organizations that took measures still turned out to have been hacked.
On 1 July 2020, security firm Fox-IT published information that it had determined that 25 Dutch servers had still been hacked via the vulnerability in the Citrix software. The organizations in question had implemented the patch, but had been penetrated before they took this action. Criminal attackers and/or state actors then had access to the internal network of these organizations. According to Dutch national newspaper de *Volkskrant*, these included a company producing watermarks for banknotes and a pharmaceutical company.[78]

3.2 Analysis of the occurrence involving Citrix software

In the analysis of the occurrence, we answer the following investigation questions:
- How could the security breaches due to vulnerabilities in Citrix software occur and what were the consequences?
- How were these risks managed by the manufacturer and organizations that used the software?
- What was the role of the government and non-government parties?

77 The computer crisis teams for the healthcare sector (Z-CERT), municipalities (Information Security Service for municipalities IBD), water authorities (CERT Water management) and education and research (SURFcert).
78 https://blog.fox-it.com/2020/07/01/a-second-look-at-cve-2019-19781-citrix-netscaler-adc/
https://www.volkskrant.nl/nieuws-achtergrond/half-jaar-na-citrix-crisis-zijn-25-nederlandse-organizaties-gehackt-en-ze-weten-zelf-van-niets

We first describe the nature of the vulnerability in the software, how it remained in the software without being discovered, and how this in turn led to a security breach in a digital system. In the subsequent sections, we analyse the factors that give meaning to the Citrix software containing this vulnerability, how the manufacturer responded to the incident, and how the incident was tackled.

3.2.1 Security breach as a consequence of the vulnerability in Citrix software

The vulnerability in the Citrix software resulted from a combination of multiple minor vulnerabilities.[79] The consequence was that at organizations that had in some way used this Citrix software in their network, *unauthorized* persons cloud have been able to move throughout the entire network, and could alter the settings in such a way that they themselves were able place software code on the network, and could then execute that code remotely. The vulnerabilities in the software made it possible for attackers to bypass security measures and to remotely execute malicious code on the network of the organization in question.

Using the vulnerability, unauthorized users (including attackers) could have been able to gain access to all components of the Citrix appliance.[80] On appliances accessible from the internet, it is common practice to configure the appliance to prevent this: the remainder of the network is then protected and is not accessible to users from outside. This can be achieved in either of two ways:

- by withholding users the possibility of giving a command to the webserver that enables them to move through all components of the appliance and thus gaining access to the protected parts of the network; and/or
- not giving users rights to view the complete directory structure.

These measures can be initiated by the organization managing the Citrix appliance, or they can be enforced by the manufacturer, through the configuration of the Citrix software. The extent to which the vulnerability could lead to a security breach depended on the standard settings in the software and how the organization using the software had restricted the rights of the users on the Citrix appliance. If the organization had not taken these measures, it was possible for an attacker to access all parts of the webserver. An unauthenticated user thereby acquired the same rights as a manager, namely access to all directories on the webserver (see figure 14 below). Not only access to view, but also to execute programmes on the network. The vulnerability that allows an attacker to operate in this way is known as *path traversal*.[81] By using the possibility of path traversal, attackers were able to bypass certain access measures and make their way into otherwise inaccessible paths and to implement programmes without authentication. However, path traversal on its own was not sufficient to read out files.

79 Fox-IT, *A Second Look at CVE-2019-19781* (Citrix NetScaler / ADC), 2020. Available via: https://blog.fox-it.com/2020/07/01/a-second-look-at-cve-2019-19781-citrix-netscaler-adc/

80 A network appliance is a type of computing appliance that aids in the flow of information to other network-connected computing devices.

81 The attacker was able to implement path traversal by entering the code '/../' in the path of the webserver.

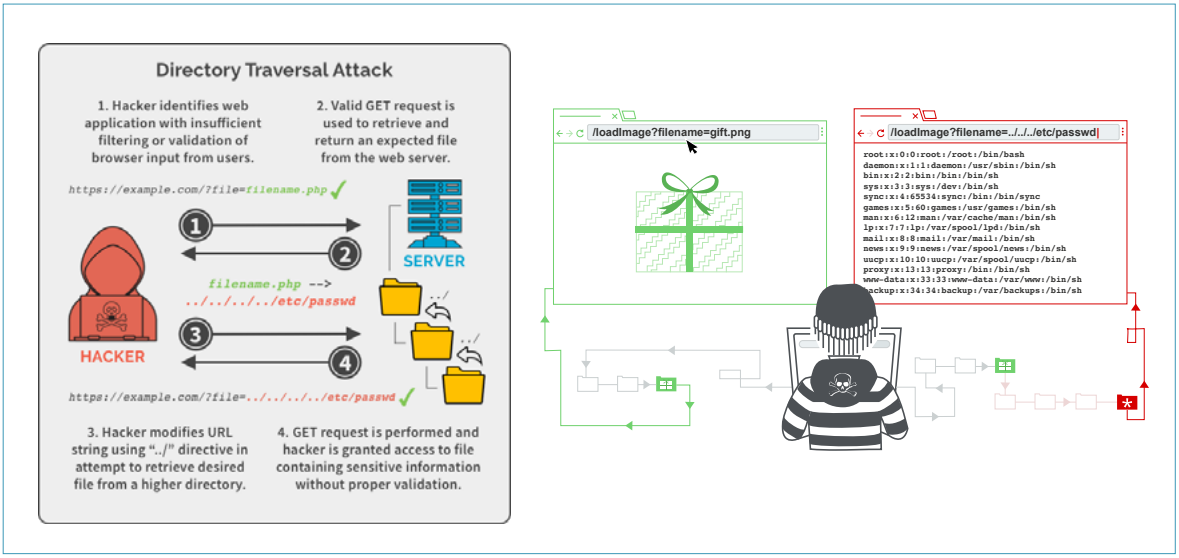

Figure 14: Directory/path traversal attack. (Source: (l) https://spanning.com/blog/directory-traversal-web-based-application-security-part-8/[82] and (r) https://portswigger.net/web-security/file-path-traversal)

3.2.2 The Citrix software had acquired a safety-critical function, over the course of time

The security breaches within organizations were partly due to the vulnerabilities in a series of software products from Citrix, namely the Citrix Application Delivery Controller (ADC). This product series has a long history. ADC is a product developed in 1997 by NetScaler, to assist companies like Google and Amazon to manage their hardware more efficiently, so that as the internet grew, the amount of hardware required remained limited. The product was based on a number of open source components. In 2005, the company NetScaler was purchased by Citrix, to fill a gap in their production line. As time went by, the manufacturer added functionalities to the product, and organizations started to implement the product in a different way. As a consequence, the product evolved to include additional functions, such as the transmission of traffic to applications and distribution across servers in the underlying network, a firewall, establishing VPN links and the authentication of users who were authorized to make use of the underlying network. Over time, the product gradually became the access gateway to the network of the organization.[83] Software that operates in a dynamic environment of this kind calls for adaptive risk management from the manufacturer. In this case, Citrix states it employs a Secure Development Lifecycle program as a key aspect of its product development framework. This issue is discussed in further detail in section 4.1.

3.2.3 Third parties discovered the vulnerability before it was found by the manufacturer

The PoC code that the security investigators shared with Citrix in December 2019 revealed a vulnerability in the ADC and Gateway. Due to the shared origin of both products, the same vulnerability was present in both products. The vulnerability in the ADC and Gateway was not yet known to the manufacturer. Security investigators do not always report a vulnerability to the manufacturer itself. A vulnerability is sometimes discovered by individual investigators or by investigators working on behalf of an

82 Spanning Cloud Apps homepage: https://spanning.com/
83 Citrix, video *The Citrix ADC story*, https://www.youtube.com/watch?v=HEWmy9-te2I, 29 November 2018.

organization using the software. Just like many other software manufacturers, Citrix encourages security investigators to immediately report vulnerabilities to them, to prevent those same vulnerabilities being sold or made available to third parties. The trade in vulnerabilities is both lucrative and non-transparent. As a result, it is possible that third parties may be aware of and exploit vulnerabilities in a software product, without the manufacturer itself having been informed. Also in this case, it was reported that the vulnerability was already circulating without Citrix' knowledge

3.2.4 Mitigating measure prior to definitive patches

As described in section 3.1, Citrix had learned from various sources that the method of exploiting the vulnerability was already circulating on certain online channels. The manufacturer therefore recognized the importance of fixing the vulnerability as quickly as possible. The Citrix response team, the first party to examine and assess reports of this kind, first contacted the *product security incident response team (PSIRT)*. This team specializes in dealing with security incidents for the various products in the Citrix portfolio. The *product R&D team* at Citrix, responsible for developing new software and patches, was then also called in. Discussions between these departments and further analysis by the R&D team revealed that a quick, permanent fix would not be achievable. Because the vulnerability was present in multiple products and multiple versions, a series of different patches had to be developed. The estimate by Citrix at that time was that several months would be needed to prepare all the patches and to work through the relevant test cycles. The manufacturer estimated that this would take so much time because the validation of security fixes of this kind demands in-depth knowledge of the product, and that a limited number of engineers with the required knowledge was available within the company.

Patches have to pass through a test cycle before they can be released to customers by the manufacturer. To repair the vulnerability, the manufacturer decided to produce a new version (*build*) of the software. This activity was expected to take several days. At that point, given the complexity of the issues and the required fixes, the manufacturer had only one team available that would be able to carry out all the automatic tests and manual validations of all patches for the different versions of the product (and because the vulnerability had been in the product line for more than ten years, there were many different versions involved). The manufacturer did not have enough engineers to be able to divide the development, testing and validation of the patches for the different versions among different teams, in such a way that all the different versions could be developed in parallel. As a result the patches for the various product versions could only be developed sequentially. Because of the time it would take to develop the patches, the manufacturer decided to take steps to mitigate the vulnerability as a measure to remedy the effect of the vulnerability.

3.2.5 Publication of mitigating measure made it simple to make an exploit

The mitigation steps advised by Citrix included information necessary for the mitigation to be implemented. Publishing information on how to implement a mitigation measure is standard practice, but may also make clear, as in this case, how the vulnerability can be exploited. The mitigating steps specified how the configuration of the webserver should be adjusted in order to prevent exploitation: make sure that the /../ command is prevented. Also, the mitigation measure disclosed where the 'path' was located so that it is clear which part of the software to look for. Publication of the mitigating steps made it clear to potential attackers that the vulnerability was related to the use of path traversal in the handling of requests (by the server).[84]

3.2.6 Manufacturer did not reach all organizations that used Citrix software

In addition to publishing the mitigation steps, the manufacturer decided to warn as many of its customers as possible, directly. At that time, the manufacturer did not yet have a possibility for contacting large groups of customers. Contact was only possible for customers who had already signed up to receive security warnings. The manufacturer only had access to the contact details of a small proportion of the organizations using its software (10%). in addition, Citrix informed us that they initiated a vast campaign to obtain as many contact details of customers as possible. For those customers whose contact details were known, the manufacturer was not sure whether the contact details were still up to date. Software manufacturers do not always know who is using their software, because the majority of sales take place via partners.

The contact details of customers to which the manufacturer did have access often proved not to be for the person responsible for security but for example the receptionist or the procurement department. The manufacturer realized that it is important to have the contact details of the person responsible for security, because otherwise there is a risk that the information about the vulnerability could end up in the wrong hands or not reach those within the organization with the responsibility and in the position to take action. Another obstacle was that certain partners do not want Citrix to contact their customers directly, and that other customers also do not want direct contact with Citrix, for example to avoid liability, in the event that an organization is contacted by the manufacturer, but doesn't take action.

3.2.7 The NCSC was unable to make inventory of the number of Dutch organizations using Citrix software and of the effectiveness of the mitigation steps

During the occurrence, organizations could be warned using information gathered by security investigators scanning the internet for servers that were still vulnerable. NCSC received most scan information from third parties like the DIVD and Bad Packets (NCSC described the scan information as 'telephone directories' because of the size of these lists). The NCSC did not scan themselves, not even the systems of its own target group organizations (national government and vital operators) because legal objections to such actions had been expressed within the organization. Also, the interpretation of the legal framework resulted into the NCSC not passing on the data to the organizations representing these groups. The NCSC informed the organizations that belonged to its own target group (national government and vital) that could be derived from these lists.

84 See for example https://northwave-security.com/threat-response-citrix-gateway-adc-rce-cve-2019-19781/

Based on a decision by the director of the NCSC, other switching organizations within the National Covering System that had not yet been designated as CERTs or OKTTs and other organizations not being national government or vital were also informed (footnote: These are therefore also personal data and/or data as referred to in Section 20(2) of the Wbni).

At a crucial moment during the incident management process, when the social and administrative situation in the Netherlands escalated on 16 January, more uncertainty emerged because Citrix wrongly announced that the mitigation steps were not always effective. As a result, the NCSC lost confidence in the mitigation steps[85] and in addition to the information from the AIVD, this played a role in formulating the far-reaching security advice to shut down the Citrix servers. Organizations reported to NCSC that the mitigation was not effective, but the NCSC was unable to independently confirm whether the organization had implemented the mitigation steps incorrectly. The NCSC had no resources to determine the reliability of the mitigating measures itself; instead it was dependent on information from third parties. The resources did exist at the department of Defense, and they were used. Security companies including Fox-IT continued to argue (also in public) that there was no reason to assume that the mitigation steps would not be effective in all cases, based on the nature of the mitigation steps that would completely eliminate the possibility of abuse and based on its own experience with customers.[86] When the patches came out, NCSC did organize to get information that would allow it to make statements about the effectiveness of the patches.

The evaluations and interviews held by the Safety Board led the Board to conclude that at a crucial moment in the incident management process (namely at the moment of issuing the security advice to shut down the Citrix servers) the NCSC failed to note that Citrix had withdrawn its earlier notice that the mitigating steps were not effective for every version of the software.

3.2.8 Organizations did not receive all the available information for their independent risk assessment

As described in section 3.1.2 after receiving the advice from the AIVD, politicians and policy makers decided that the NCSC would urgently advise Citrix servers to be shut down. The NCSC operated on the basis of the principle that organizations were first and foremost responsible for making their own risk assessment, because they could determine whether or not implementing security measures had an impact on the security or the continuity of operations. The organizations wanted to know what additional information the urgent security advice from the NCSC was based on, as compared with the previous advice. They needed this information to make a risk assessment based on their own specific circumstances. It was relevant for them whether the new information was related to a specific threat against a particular organization, or whether it was a precautionary measure.

85 The NCSC indicated it had lost confidence in the mitigation measures due to messages received from users and confirmation from Citrix that the measures did not work for at least one version. Citrix states that they immediately retracted the message and that they know of no cases where the measures did not work.

86 Fox-IT, *Advisory on Citrix vulnerability*, 17 January 2020. "Based on all the current rumors and speculations about the Citrix vulnerability, we decided to list all the current known facts in an advisory."

All government organizations were required to inform CIO Rijk whether they had taken measures. The NCSC, the Minister of the Interior and Kingdom Relations and the policy departments of the Minister of Justice and Security also approached organizations that were not part of national government, and were not considered vital operators such as large municipalities and care institutions, with the request to comply with the urgent security advice from the NCSC. Organizations subject to multiple legal regimes (large telecom providers for example) were approached by multiple parties, causing them additional burden, while at the same time they had to fight the crisis. On 23 January 2020, the Minister of Justice and Security and the Minister of the Interior and Kingdom Relations organized a technical briefing for the Dutch House of Representatives, together with the NCTV deputy and the director of the NCSC.[87]

Different organizations consulted by the Safety Board indicated that despite believing that they had correctly implemented all the recommended mitigation steps, they still felt they had to shut down their systems as a precaution. The reason was that they were experiencing administrative pressure, and did not know what information the MIVD and AIVD had issued to the NCSC, nor what the purport of the advice was. The organizations were dependent on the NCSC and the AIVD for this information; they had no possibility of obtaining the information by themselves. The NCSC believed that it was not in a position to pass on this information to organizations outside national government.

3.3 Course of events of other illustrative occurrences

The occurrence where vulnerabilities in Citrix software led to security breaches in organizations is not an isolated event. In this section, we describe other occurrences involving software that fulfils a comparable function as the Citrix software (granting remote access to a digital system at an organization) and whereby vulnerabilities in this software had consequences for the cybersecurity of those organizations. The vulnerabilities that are addressed in this investigation are at present still among the vulnerabilities that are most commonly used in attacks.[88]

87 The Dutch House of Representatives was also one of the organizations that used Citrix and that had shut down its systems.

88 CISA, *Top Routinely Exploited Vulnerabilities* (thus far in 2021), 28 July 2021. https://us-cert.cisa.gov/ncas/alerts/aa21-209a

Outages, accidents and attacks

In this section, we describe occurrences whereby vulnerabilities lead to attacks on organizations. Vulnerabilities in software can however also threaten the security of digital systems in other ways, thereby causing damage and injuries. In June and July 2021, for example, a large number of websites worldwide became inaccessible for a short period of time: newspapers, media, online stores, banks, cloud services and government services, such as the 911 emergency number in parts of the United States and the government domain in the United Kingdom. In both cases, the outage was caused by an error in the software of an Internet service provider used by multiple organizations to improve the speed and stability of Internet traffic to their websites. Software is not only used in digital systems but is also embedded, for example in vehicles, aircraft and chemical installations. Vulnerabilities in software, in combination with other factors, can in such situations lead to an accident.[89] In these cases, coincidence plays a greater role than in the event of attackers exploiting vulnerabilities and thereby using automated systems to identify all servers containing the vulnerability.

3.3.1 VPN software for the enterprise market[90]

Organizations use (enterprise) VPN software to give their employees a remote secure link and access to the company network. As with the Gateway software from Citrix, these VPN products fulfil a central role in the security of the underlying network. A small number of manufacturers dominate the market for these professional VPN products. Pulse Secure, for example, is used in more than 50,000 servers connected to the internet worldwide, in particular for large companies and governments; Fortinet is used by more than 480,000 internet-faced servers worldwide, especially by medium-sized organizations.[91] The number of servers using Palo Alto software is unknown to the Dutch Safety Board.

The search for vulnerabilities

In 2018 security investigators had noticed that until that time, relatively few vulnerabilities in certain enterprise VPN products had been published as compared with other comparable products. They wondered whether this was because the products contained so few vulnerabilities, or because despite their crucial role for the security of digital systems, these products represented a blind spot (in that little action was taken to search for vulnerabilities in these products). For that reason, in 2019 they went in search of vulnerabilities in VPN products from Fortinet, Palo Alto and Pulse Secure.

89 Outage internet service providers: https://www.fastly.com/blog/summary-of-june-8-outage and https://www.reuters.com/technology/websites-airlines-banks-tech-companies-down-widespread-outage-2021-07-22/
See for example a recall by Fiat Chrysler, due to a software vulnerability that meant that airbags were not activated in certain accidents. https://www.reuters.com/article/us-fiatchrysler-recall-idUSKBN1881I6

90 VPN stands for Virtual Private Network.
CVE 2019-11507/10 multiple vulnerabilities in Pulse Secure software (seriousness varying from 6 to 9 on a scale of 1 to 10).
CVE 2018-13379 vulnerability in Fortinet software (seriousness 9.8 on a scale of 1 to 10).
CVE 2019-1579 vulnerability in Palo Alto software (seriousness 8.1 on a scale of 1 to 10).

91 https://techcrunch.com/2019/07/23/corporate-vpn-flaws-risk/

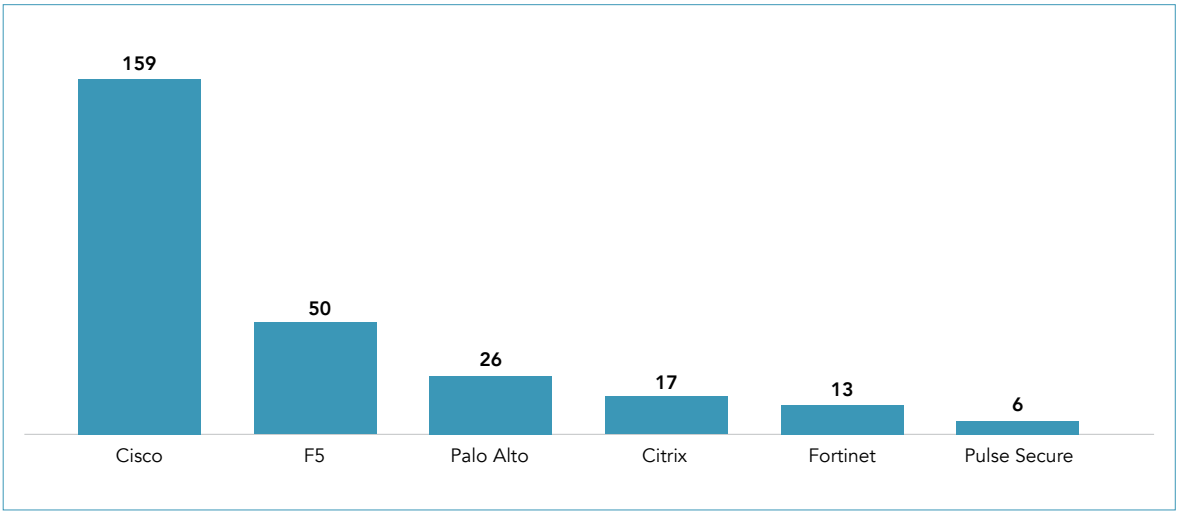

Figure 15: Analysis by security researchers of vulnerabilities in VPN products by the security investigators (no indication is given of the period to which this analysis relates). (Source: Blog of the security researchers)[92]

One obstacle for the security investigators was that the products are closed source. After breaking open the software (a process known as a jailbreak), they found a number of vulnerabilities. The most important vulnerability within the Pulse Secure product occurred after a new functionality had been added to the product in 2016 in version 8.2.

The security investigators reported the vulnerabilities first to the manufacturers and to the owners of the compromised company networks. They then shared their findings in technical journals, at conferences and on their own blog.[93] The incident response by the affected manufacturers varied: Pulse Secure published the vulnerability and a patch one month following the report by the security investigators. A month following the warning, the security investigators used the vulnerability to successfully penetrate Twitter. Fortinet dealt with its vulnerability after 7 weeks, and states to have published a warning at the same time. Palo Alto initially announced that it would not be publishing a warning, because it was already aware of and had repaired the vulnerability. After the security investigators had successfully penetrated Uber via the vulnerability in Palo Alto and had published about their activities, the manufacturer went on to publish a warning.

Between one day and one month after the security investigators had demonstrated how they could exploit the vulnerabilities in the software, it became apparent that attackers were actively scanning the internet for servers on which this vulnerability in the software had not yet been repaired with a patch. At that moment, many dozens of Dutch organizations had not yet implemented the update, including KLM, Shell, Boskalis, various defence-related companies, the Ministry of Justice and Security and Air Traffic

92 https://blog.orange.tw/2019/08/attacking-ssl-vpn-part-2-breaking-the-fortigate-ssl-vpn.html
93 https://www.defcon.org/html/defcon-27/dc-27-speakers.html#Tsai
https://i.blackhat.com/USA-19/Wednesday/us-19-Tsai-Infiltrating-Corporate-Intranet-Like-NSA.pdf
https://devco.re/blog/2019/07/17/attacking-ssl-vpn-part-1-PreAuth-RCE-on-Palo-Alto-GlobalProtect-with-Uber-as-case-study/,
https://devco.re/blog/2019/08/09/attacking-ssl-vpn-part-2-breaking-the-Fortigate-ssl-vpn/
https://devco.re/blog/2019/09/02/attacking-ssl-vpn-part-3-the-golden-Pulse-Secure-ssl-vpn-rce-chain-with-Twitter-as-case-study/ Message Pulse Secure
https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101

Control the Netherlands (LVNL). Most of these organizations implemented the update after August 2019.[94]

In August 2020, it was announced that attackers had compiled a list of stolen user names, passwords and IP addresses from around 900 vulnerable Pulse Secure VPN servers. The data appeared to have been collected between 24 June and 8 July 2020. The list was published on a forum commonly visited by ransomware gangs. In the summer of 2021, something similar happened: on an newly launched hacker forum, attackers published - possibly as a publicity stunt - a list of 500,000 login credentials for Fortinet VPN servers. These credentials were allegedly collected from servers still vulnerable to the vulnerability described in this section.[95] According to Fortinet of these numbers ultimately 140,000 credentials and 24,000 devices turned out to be exploitable.

In the months and years after publishing the vulnerabilities various national CERTs, including the American national cybersecurity agency CISA, and also the Dutch intelligence and security services, issued repeated warnings that various attackers, including state actors were exploiting vulnerabilities in the software to launch attacks on the digital systems of organizations.[96] The vulnerabilities in the software, just like the vulnerabilities in the Citrix software, had thereby become part of the international arsenal of cyberweapons.

94 Modderkolk, H., Intern netwerk honderden bedrijven en ministerie lang maandenlang wagenwijd open (title translates: Internal network hundreds of companies and ministry wide open for months), *Volkskrant* newspaper of 28 September 2019. Parliamentary Papers II 2019-2020, 26 643, no. 666 'Analysis of risks run due to the vulnerabilities in the virtual private network (VPN) software from the company Pulse Secure'. NCTV, Cybersecurity picture 2020, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2020Z02670&did=2020D05619, https://blog.cyberwar.nl/2019/09/dutch-kwetsbare-pulse-connect-secure-ssl-vpn-in-nederlandse-ip-adresruimte-bevindingen-en-gedachten/ Koot, M., *Field Note on CVE-2019-11510: Pulse Connect Secure SSL-VPN in the Netherlands*.In: Digit. Threat.: Res.Pract.1, 2, Article 13, May 2020. https://dl.acm.org/doi/10.1145/3382765

95 https://www.zdnet.com/article/hacker-leaks-passwords-for-900-enterprise-vpn-servers/ (August 2020). https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/ (September 2021).

96 https://us-cert.cisa.gov/ncas/alerts/aa20-258a *Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity.*
https://us-cert.cisa.gov/ncas/alerts/aa20-259a *Iran-Based Threat Actor Exploits VPN Vulnerabilities*, https://ics-cert.kaspersky.com/reports/2021/04/07/vulnerability-in-fortigate-vpn-servers-is-exploited-in-cring-ransomware-attacks/, https://www.security.nl/posting/697797/FBI+waarschuwt+voor+misbruik+van+Fortinet+FortiOS-kwetsbaarheden

From vulnerability to cyberweapon in less than a week

In the summer of 2020, it became known that the BIG-IP software from the company F5 contained a vulnerability. This product fulfils a similar function to the previously described Citrix software. The product consists of various modules such as Local Traffic Management, DNS, access policy, firewall. On 30 June 2020, F5 announced that the management interface of the Traffic Management module in BIG-IP contained a vulnerability. On servers on which the management interface was connected to the internet, attackers without legitimate credentials could execute arbitrary malicious code on the server, thereby penetrating the digital system behind this module. The vulnerability was so serious that it was given a score of 10 on a scale of 1 to 10. This vulnerability caused considerable unrest, since it was announced just before the weekend of the 4th of July, a period in which many Americans have time off work. This hindered the timely patching of the vulnerability. Five days after F5 published the vulnerability, a security investigator had also published a method for exploiting the vulnerability. The method was so simple that the necessary code fitted in a single Tweet. Two days later, organizations using BIG-IP worldwide suffered attacks.[97]

Incident management

At the time of the vulnerabilities in Pulse Secure, Fortinet and Palo Alto, the DIVD had not yet been established. On his own initiative, one Dutch security investigator scanned the internet for servers containing the vulnerable Pulse Secure and Fortinet software, and passed this information on to the NCSC. The security researchers had also found vulnerable servers outside this target group. NCSC did not warn these organizations, without informing the security researchers. As with the Citrix incident, the legal frameworks were interpreted to allow NCSC to share this data in a limited way. Based on a decision by the director of the NCSC, other switching organizations were also informed, namely: organizations within the National Covering System that had not yet been designated as CERT or OKTT and other organizations not being national government or vital. These received personal data and/or information as referred to in Article 20, paragraph 2, Wbni. This was done on the basis of the potential social impact or on the grounds of social importance.

Months later, the vulnerabilities still continued to have consequences for the organizations using the software, even if in the meantime they patched the vulnerabilities. On 4 August 2020, for example, attackers of Pulse Secure servers published details they had obtained during attacks on more than 900 Pulse Secure servers. The information included login data of server managers (admin account details) and all user names and passwords of the local users.[98] In the meantime the DIVD had been established. On 5 August, the DIVD sent out warnings to the organization connected to the Dutch IP addresses appearing on this list.

97 Notice from F5: https://support.f5.com/csp/article/K52145254
https://www.bleepingcomputer.com/news/security/poc-exploits-released-for-f5-big-ip-vulnerabilities-patch-now/
and https://www.bleepingcomputer.com/news/security/us-govt-confirms-active-exploitation-of-f5-big-ip-rce-flaw/

98 https://csirt.divd.nl/cases/DIVD-2020-00009/

On 19 November 2020, a security investigator came across a list of 49,577 vulnerable Fortinet servers on the Internet, and the magazine Bleeping Computer published an article on this finding, on 22 November. On 25 November 2020, the DIVD started examining the list for Dutch organizations. Starting on 3 December 2020, The DIVD sent out the first warnings to these organizations.[99]

3.3.2 Wave of cyber-attacks via software vulnerabilities and supply chain attacks

The events described in the previous subsection were the precursor to a worldwide wave of cyber-attacks and data breaches via software vulnerabilities, whereby attackers also made use of security breaches at service providers to attack other organizations. This is a phenomenon known as *supply chain attacks*.

SolarWinds/SUNBURST

The escalation of cyberattacks started with the discovery of the SolarWinds/SUNBURST attack in December 2020. The Washington Post wrote on 13 December 2020 that various American governments had been hacked via the Orion software from the company SolarWinds. The attack was attributed to the Russian government. One security company had discovered that attackers had added malicious code to the software updates from SolarWinds, allowing attackers to gain access to all customers that had implemented the software update. Among the SolarWinds customers were American government organizations, major companies (including the security company that discovered the attack), NATO, the European Parliament, AstraZeneca and government organizations in the United Kingdom.[100]

Microsoft Exchange

Following the SolarWinds/SUNBURST attacks, four zero-day vulnerabilities were discovered in local installations of Microsoft Exchange server. Servers with these vulnerabilities suffered attacks, worldwide. These attacks were reported to Microsoft by security investigators. A link was suspected with the previous SolarWinds attack (it was alleged that the attackers had gained access to the source code for the software at Microsoft) but this has not been confirmed. Microsoft attributed the attack to an attack group backed by the Chinese government that targets infectious disease researchers, law firms, educational institutions and defense contractors. On 2 March 2021, patches were published, to fix the vulnerability. However, these patches were not able to rectify the damage or to remove the backdoors the attackers had already installed.[101]

99 https://csirt.divd.nl/cases/DIVD-2020-00012/

100 "Russian government spies are behind a broad hacking campaign that has breached U.S. agencies and a top cyber firm". *The Washington Post*. December 13, 2020. Gallanger, Ryan, Donaldson, Kitty, et al. (15 December 2020). "U.K. Government, NATO Join U.S. in Monitoring Risk From Hack". *Bloomberg News website*. Sanger, David E.; Perlroth, Nicole; Schmitt, Eric (December 15, 2020). "Scope of Russian Hack Becomes Clear: Multiple U.S. Agencies Were Hit". *New York Times*.

101 https://en.wikipedia.org/wiki/2021_Microsoft_Exchange_Server_data_breach#cite_note-Microsoft-CVE-3

'Cheese hack'
One of the companies attacked via the vulnerability in Microsoft Exchange was a Dutch logistic service provider. The attack shut down part of the dairy distribution chain, including the supply of cheese to supermarkets. As a result, this attack campaign in the Netherlands was given the nickname 'the cheese hack'.[102]

It is estimated that on 9 March 2021, 250,000 servers worldwide had become victims of these attacks, both in the US and in Europe. In the US, the attack was judged as being 1,000 times more harmful than the SolarWinds attack in December 2020, in terms of economic damage. This was because the Exchange attack affected large numbers of small and medium-sized enterprises, a driving force for the economy. In the US, at least 30,000 organizations had been hacked as a result of the vulnerability, by the start of March 2021. On 22 March 2021, Microsoft announced that 92% of the servers had been patched or mitigated.[103]

On 3 March 2021, the DIVD in the Netherlands started scanning for vulnerable servers in the Netherlands and the rest of the world. On 4 March, the DIVD sent a list of Dutch IP addresses to the NBIP, for notification. In total, the DIVD sent out more than 42,000 warnings. Later in March, they once again scanned for and warned Dutch organizations. By that time, around 15,000 servers were still vulnerable; in May there were still 7,000 vulnerable servers, in addition to a further 5,500 servers that contained vulnerabilities that were published in April.[104]

Tension between Microsoft and security investigators
Reports were published on 15 March 2021 that the exploit code submitted to Microsoft on 5 January 2021 may have been leaked and used by attackers. The media reported that this had led Microsoft to investigate the partner companies that had received early information about the vulnerabilities and patches. On that same day, reports suggested that there was unrest among security investigators because at the request of Microsoft (owners of GitHub), GitHub had deleted the code of an exploit. GitHub subsequently changed its terms and conditions, allowing GitHub to intervene to prevent the platform being exploited for the exchange of attack methods used in attack campaigns.[105]

102 https://nos.nl/artikel/2376492-oproep-na-kaas-hack-bestempel-voedselvoorziening-als-vitale-infrastructuur, Marc Hijink, "De les van het lege kaasschap" (The lesson learned from the empty cheese shelf), *NRC*, 2021. "Duizenden extra Exchange-servers kwetsbaar" (Thousands of additional Exchange servers vulnerable), *AG Connect*, 2021, consulted on 17 March 2021, https://www.agconnect.nl/artikel/duizenden-extra-exchange-servers-kwetsbaar.
103 https://www.techrepublic.com/article/how-the-microsoft-exchange-hack-could-impact-your-organization/
104 https://csirt.divd.nl/2021/05/14/Closing-ProxyLogon-case/
105 https://www.agconnect.nl/artikel/exchange-exploit-lijkt-uitgelekt-bij-melding-aan-microsoft, https://www.agconnect.nl/artikel/rel-na-wissen-exchange-exploit-door-github and https://www.theregister.com/2021/03/12/github_disappears_exploit/, https://thehackernews.com/2021/06/github-updates-policy-to-remove-exploit.html

Kaseya VSA software

July 2021 saw a new wave of cyber-attacks. Once again in the 4th of July weekend, hundreds of companies were attacked, worldwide. On this occasion, the attack was attributed to a Russian ransomware gang. In April 2021 Dutch security investigators affiliated to the DIVD had informed the company Kaseya that they had discovered vulnerabilities in Kaseya's VSA software. This software was used by IT service providers (also known as managed service providers or MSPs) for the remote management of their customers' digital systems and sometimes also by the companies themselves.. Before Kaseya was able to patch these vulnerabilities, the ransomware gang had launched its worldwide attack campaign. In Sweden, the attack led to a supermarket chain with 800 stores being forced to close its doors. Not because the supermarket itself had been affected via the Kaseya software, but because the company responsible for payment systems in the supermarkets had been attacked.[106]

3.3.3 Urgency and scale of unsafety constantly growing

The occurrences we describe in this chapter show that vulnerabilities continue to be widely exploited to carry out attacks and that new vulnerabilities constantly emerge. Vulnerabilities in software are therefore an increasingly urgent and serious threat to the digital security and safety of organizations.[107]

When a vulnerability in software is identified, organizations have ever less time to mitigate or patch the vulnerability before vulnerable servers suffer attacks, worldwide (see Annex D). This threat has further escalated over the past twelve months, because both criminal attackers and state actors are increasingly opting to launch their attacks via supply chain partners. Via supply chain attacks of this kind, attackers can hack into an organization's supply chain, literally via its weakest link. As a result, attacks can escalate in scale, while the potential for response of individual organizations to protect themselves against attacks via a supply chain partner is diminishing.

What the occurrences also demonstrate is that volunteer security researchers, such as through DIVD, played a crucial role in the response to the incident and information sharing. Indeed, they scanned the entire Dutch (and global) domain, which provided them with the necessary information to identify which organizations had not yet fixed the vulnerability and to warn these organizations...

106 After talks between President Biden and Putin, this ransomware gang disappeared from view for a time. Some see this as proof that it is effective to take (diplomatic) action internationally after cyberattacks from another country. https://nos.nl/artikel/2387973-nederlandse-ethische-hackers-probeerden-ransomware-aanval-te-voorkomen; "Swedish Coop supermarkets shut due to US ransomware cyber-attack," *BBC*, 2021, consulted on 4 July 2021, https://www.bbc.com/news/technology-57707530

107 CISA, Top Routinely Exploited Vulnerabilities, 28 July 2021. https://us-cert.cisa.gov/ncas/alerts/aa21-209a