citrix

Minister of Economic Affairs and Climate Policy
PO Box 20401
2500 EK Den Haag
Netherlands

RE: Response to Onderzoeksraad voor Veiligheid, “Kwetsbaar door software”, d.d. 16-12-2021

June 24, 2022

To the Minister of Economic Affairs and Climate Policy,

On December 16, 2021, the Dutch Safety Board (“DSB”) published its finalized report titled “*Vulnerable Through Software*” (hereafter: the “Report”), which investigated software vulnerabilities and the impact thereof in the Netherlands.

In the Report, the DSB makes two recommendations[1] relevant to software manufacturers:

1. *Develop good practices with other manufacturers to make software safer and more secure. Include a commitment to these practices in contracts with your customers.*

2. *Warn and help all your customers as quickly and effectively as possible when vulnerabilities in software are identified. Create the preconditions necessary to be able to warn your customers.*

Pursuant to Art. 74 of the Dutch Safety Board Act, Citrix hereafter summarizes how it addresses these recommendations by the DSB.

1. Development of good practices with other manufacturers

As part of its commitment to the development of secure software, Citrix participates in a number of technology industry and industry-government initiatives aimed at the maintenance and improvement of the security of software and computing environments. These include memberships in the Center for Internet Security (Product Vendor member); the Xen Community Board (three board members); and the Cloud Security Alliance Bangalore Working Group (Research Member). Citrix also participates with other technology providers[2] in the Cybersecurity Coalition[3], whose mission is to bring together leading companies to help drive policy solutions around the improvement of cybersecurity. And in response to the recent series of well-publicized ransomware incidents throughout the industry, Citrix joined the Institute for Security & Technology’s Ransomware Taskforce[4], whose participants include a broad representation of software manufacturers as well as the U.K. National Cyber Security Centre (NCSC)[5] and the U.S. Cybersecurity & Infrastructure Security Agency[6].

In addition to Citrix’s participation in these groups, we strongly favor standards-based cybersecurity requirements for manufacturers. Standards-based cybersecurity requirements lead to more effective market standards because they are more broadly adopted, thereby increasing the cybersecurity posture across a wider surface. In that regard, Citrix notes that it already abides by well-established cybersecurity

[1] Page 123 of the Report.
[2] See here for a list of member companies: https://www.cybersecuritycoalition.org/#member-companies
[3] https://www.cybersecuritycoalition.org/
[4] https://securityandtechnology.org/ransomwaretaskforce/
[5] https://www.ncsc.gov.uk/
[6] https://www.cisa.gov/

standards like the NIST[7] and ISO[8] norms. ISO, for example, maintains a comprehensive standard (ISO/IEC standard 29147:2018) with respect to vulnerability remediation and response, which Citrix adopted and against which it regularly audits itself. And more generally, Citrix evaluates it products and services against standards under ISO, Common Criteria[9], and SOC2[10], and publishes certifications on its Trust Center.[11] The frameworks provided by independent standards-setting organizations are more likely to lead to a broader adoption across the industry than inviting competing efforts amongst selective manufacturers.

Citrix, of course, is open to further industry initiatives and will consider these as and when appropriate in order to further enhance the security of the software market.

2. Warning of and support to customers in respect of vulnerabilities

As Citrix indicated in its responses during the DSB's investigation, Citrix is dedicated to delivering secure software to its customers and relies on its internal Secure Development Lifecycle (SDL) process to minimize the risks to our customers. As part of the SDL process, Citrix takes a comprehensive approach to investigating, addressing and informing customers of any known product vulnerabilities. Citrix maintains a number of processes aimed at ensuring that customers are adequately informed about vulnerabilities once mitigated or fixed.

Publication of security bulletins

Citrix publishes security bulletins to provide remediation information about security vulnerabilities in customer-managed Citrix products which have been reported to Citrix through Citrix's vulnerability response program. Citrix may also publish security bulletins to inform customers of other important events affecting Citrix products. For example, if a critical third-party CVE (under MITRE's Common Vulnerabilities and Exposures program) impacts a Citrix product and has gathered significant public attention. Citrix will usually publish a security bulletin once software patches or mitigations exist for all versions of a product that have not yet reached End of Maintenance. In limited circumstances, including where Citrix has observed active exploitation of a vulnerability or where public awareness of a vulnerability could lead to increased risk for Citrix customers, a security bulletin may be published before a complete set of patches have been released so that we may alert customers and provide advice on how to mitigate the associated risks. For the safety of our customers, and particularly to avoid zero-day attacks on our customers, Citrix does not disclose technical details about vulnerabilities beyond what is contained in the bulletin and does not publicly disclose vulnerabilities prior to mitigations or fixes being available. For further information about the publication of Security Bulletins, see https://www.citrix.com/about/trust-center/vulnerability-process.html

Pre-notifications for certain customers

Citrix maintains a security pre-notification program that is available to a range of customers and partners, including those in critical infrastructure, who meet certain criteria. Pre-notifications do not contain information that could be used to compromise other customers. Citrix recommends that customers apply security fixes/patches as soon as possible following their release. For further information about Citrix' pre-notification program, see https://www.citrix.com/about/trust-center/vulnerability-process.html

Patch Tuesdays
Commensurate with industry practice, Citrix typically publishes security bulletins on the second Tuesday of a month, to help customers plan to perform any applicable updates.

[7] https://www.nist.gov/
[8] https://iso.org/
[9] https://www.commoncriteriaportal.org/
[10] https://soc2.co.uk/
[11] https://www.citrix.com/about/trust-center/privacy-compliance/

Maintaining up to date mailing lists and contact details

Citrix continues to encourage users of Citrix software to provide Citrix with dedicated security contacts that can be contacted as and when needed. Citrix observes, however, that the initiative for these actions rests with customers. It will continue to look for ways to raise awareness around the registration process and encourage customers to maintain and update their security contact details with Citrix.

Availability of call home function

Citrix offers a "call home" function for equipment, whereby the device itself registers its version and updates with Citrix cloud servers. This allows Citrix to maintain an up-to-date overview of the software versions customers are running. Although Citrix plans to enhance its call home product functionality and related processes, Citrix notes that the current call home function is voluntary and requires the customer's proactive participation. For further information on the call home functionality, see https://www.citrix.com/community/cx/call-home.html.

Additional Customer Support

Citrix and its extensive partner community also provide additional resources that can help customers and users when software vulnerabilities are identified. Citrix's customer success offerings include several variations of customer and user support. Depending on the level of support selected, the customer receives technical support, training and education, expert guidance, and proactive monitoring. More information is available here.

In addition to hands-on support, Citrix provides all customers and users with extensive product documentation, which is available at https://docs.citrix.com. Citrix provides product manuals, knowledge-based articles and secure deployment guides.

Citrix also maintains the Citrix Trust Center to provide security-related information to our customers. The Trust Center provides product and service documentation; information on our vulnerability management and release processes; security and other documentation; and privacy and compliance materials. See https://www.citrix.com/about/trust-center/.

Citrix continues to look for ways in which it can further optimize its ability to quickly and efficiently warn and support customers regarding software vulnerabilities.

Citrix would like to thank the Dutch Safety Board for its efforts in producing the Report, and for formulating the recommendations in the Report. Citrix is confident that the Report and the recommendations will contribute to a strengthening of the cybersecurity resilience in the Netherlands.

Kind regards,

Robert Calderoni (Jun 25, 2022 05:07 EDT)

Bob Calderoni
Interim President and Chief Executive Officer

cc: Dutch Safety Board

851 Cypress Creek Road, Fort Lauderdale, FL 33309, USA
954 267 3000 Phone
800 424 8749 Toll Free
citrix.com

Citrix Response to DSB Recommendations

Final Audit Report 2022-06-25

Created:	2022-06-24
By:	Melissa Boudreau (melissa.boudreau@citrix.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAWvVyamF3Ncp5g0bmBUKulh9O9eNbpxD_

"Citrix Response to DSB Recommendations" History

Document created by Melissa Boudreau (melissa.boudreau@citrix.com)
2022-06-24 - 2:54:55 PM GMT- IP address: 108.20.211.116

Document emailed to bob.calderoni@citrix.com for signature
2022-06-24 - 2:55:43 PM GMT

Email viewed by bob.calderoni@citrix.com
2022-06-25 - 9:06:36 AM GMT- IP address: 69.116.211.25

Document e-signed by Robert Calderoni (bob.calderoni@citrix.com)
Signature Date: 2022-06-25 - 9:07:51 AM GMT - Time Source: server- IP address: 69.116.211.25

Agreement completed.
2022-06-25 - 9:07:51 AM GMT