Brussels, June 16, 2022

Dear Secretary Director Verheij,

On behalf of our Chairman, I would like to thank the Dutch Safety Board for contacting BSA | The Software Alliance (BSA) in relations to the Board's report "Vulnerable through Software – Lessons resulting from security breaches relating to Citrix software," released on 16 December 2021.

BSA represents the global enterprise software industry.[1] The Citrix company was not a member of BSA at the time of the incidents investigated by the Board, nor was it a member during the Board's investigation. However BSA supports the overall objective of the Board's investigation to increase digital security in the Netherlands (and beyond) and appreciated an opportunity, after a draft report had been finalized, to provide input to the Board. To that effect, BSA shared two documents containing our recommendations on software security from an enterprise software industry perspective:

- The BSA Secure Software Framework[2] proposes a risk-management approach to software security throughout the software life-cycle;
- The BSA Cybersecurity Agenda[3] includes some recommendations on software security among others.

We noted that the report addresses two recommendations to software manufacturers collectively and BSA, as follows:

> ***Recommendation 1 (page 17):***
>
> *To software manufacturers collectively:*

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry. Its members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernize and grow. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. BSA's members include: Adobe, Akamai, Atlassian, Autodesk, Bentley Systems, BlackBerry, Box, Cloudflare, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, and Zoom.

[2] BSA Secure Software Framework https://www.bsa.org/reports/updated-bsa-framework-for-secure-software

[3] BSA Cybersecurity Agenda https://bsacybersecurity.bsa.org/

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.*

Note: The responsibility and possibilities for making software safer and more secure, and for warning customers primary lies with the manufacturers themselves.

Recommendation 2 (page 123):

To software manufacturers collectively:

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.*

Note: The responsibility and possibilities for making software safer and more secure, and for warning customers primary lies with the manufacturers themselves.

BSA takes note of these recommendations and would like to offer additional comments in response.

Software development today relies on software libraries that can be purchased or on open source software. In either cases, the code can and will be modified before the software is deployed or as it is patched and maintained. A software product may also change continually and substantially over its lifecycle (because of iterative approaches to development, third-party components, evolving security threats). Therefore it becomes very complex to trace a code all the way at its inception, when it is used by customers through their own supply-chain.

Moreover, software security is not straightforward. Software products currently average roughly 1–5 defects per 1,000 lines of code, with many complex software products incorporating tens or hundreds of millions of lines of code in total. While defect-free code should always be a developer's goal, it is not a realistic industry standard.

The security of a software depends on its deployment, integration, maintenance, environment, organization's internal security and privacy policies, etc. Control over these parameters lies more often than not with the customers, not the software manufacturers. Responsibilities should therefore be established according to entities' ability to analyze, address and respond to the risks, at a given time in the software life-cycle, from a contractual, legal and technical standpoint.

Finally, with regards to informing customers and supply-chain stakeholders, it is worth noting that Coordinated Vulnerability Disclosure is well-developed within the industry.[4] There are established means for providing structured identifiers for vulnerabilities which are in use globally today in cybersecurity products and services, such as the Common Vulnerabilities and Exposures[5] program

[4] BSA's Guiding Principles For Coordinated Vulnerability Disclosure

[5] As of this writing, there are 156 organizations from 26 countries participating in exchanging vulnerability information in a structured fashion. Currently organizations in Austria, Belgium, Denmark, Finland, France, Germany, Ireland, Latvia, Netherlands, Norway, Romania, Spain, and Switzerland are participating successfully in the CVE Program.

which is a widely utilized international mechanism to address vulnerabilities and efficiently track down timely information.[6]

In conclusion, the goal of software security policies and recommendations should be the widespread adoption of practices and processes that minimize code defects, and particularly known software vulnerabilities, and to maintain a proactive security posture oriented to identifying and addressing problems before they can be exploited. The BSA Secure Software Framework was designed to help stakeholders in the software industry – developers, vendors, customers, policymakers, and others – communicate and evaluate security outcomes associated with specific software products and services. We believe it is an important resource for supporting this goal.

We look forward to continue engaging on these important issues and remain at your disposal for further discussion.

Sincerely,

Thomas Boué
Director General, Policy – EMEA
BSA | The Software Alliance

[6] https://cve.mitre.org/