Citrix and FireEye Mandiant Launch Indicator of Compromise Scanner

Free tool provides assessment of system compromise in connection with CVE-2019-19781

FORT LAUDERDALE, Fla. and MILPITAS, Calif. – Citrix Systems, Inc. (NASDAQ: CTXS) and FireEye Inc. (NASDAQ: FEYE) today announced the launch of a new tool for detection of compromise in connection with the previously announced CVE-2019-19781 vulnerability, which affects certain versions of Citrix Application Delivery Controller (ADC), Citrix Gateway, and two older versions of Citrix SD-WAN WANOP. This tool is freely accessible in both the Citrix and FireEye GitHub repositories.

The free tool is designed to allow customers to run it locally against their Citrix instances and receive a rapid assessment of potential indications of compromise in their systems based on known attacks and exploits. The tool is compatible with all supported versions of Citrix ADC and Citrix Gateway, including 11.1, 12.0, 12.1, 10.5, and 13.0, and Citrix SD-WAN WANOP versions 10.2.6 and 11.0.3. In addition to applying the previously released mitigation steps and installing the permanent updates being made available throughout this week, Citrix and FireEye strongly recommend that all Citrix customers run this tool as soon as possible to increase their overall level of awareness of potential compromise and take appropriate steps to protect themselves.

Citrix announced the CVE-2019-19781 vulnerability along with mitigations on December 17, 2019. Exploits – tools to take advantage of the vulnerability – were published by multiple third parties in early January 2020. As a result, the risk to unmitigated customer systems rose significantly.

“While our security and engineering teams have been working around the clock to develop, test and deliver permanent fixes to CVE-2019-19781, we have been actively thinking of ways to assist our customers in understanding if and how their systems may have been affected,” said Fermin J. Serna, Citrix’s Chief Information Security Officer.

“We partnered with FireEye Mandiant, which is at the forefront of cyber threat intelligence and forensic analysis, to develop a tool that leverages their knowledge of recent attacks against CVE-2019-19781 to help organizations identify potential compromises. The tool utilizes our technical knowledge of the Citrix ADC and Gateway products and CVE-2019-19781, combined with industry-leading expertise in cyber forensics and recent FireEye frontline learnings from CVE-2019-19781 related compromises,” Serna said.

Charles Carmakal, Chief Technology Officer of FireEye Mandiant consulting, said, “As we worked closely with various Citrix customers in their response to CVE-2019-19781, we developed an understanding of the active threats related to this vulnerability. We believe it is in the best interest of Citrix customers using affected product versions and the entire security community for us to join forces with Citrix to offer a free tool that organizations can rapidly deploy in their own environments to identify potential indicators of compromise of their systems.”

This tool is designed to provide increased awareness regarding potential indicators of compromise related to CVE-2019-19781 on an organization’s systems. The tool is not guaranteed to find all evidence of compromise, or all evidence of compromise related to CVE-2019-19781. If indications of compromise are identified on systems, organizations should perform a forensic examination of the compromised system to determine the scope and extent of the incident.

Instructions on how to use the tool can be found on the aforementioned GitHub sites.

Information regarding permanent fixes and mitigation steps released by Citrix in relation to the CVE-2019-19781 vulnerability can be found on Citrix’s website.

Citrix has provided additional context for customers regarding the forensic assessment tool in the following blog post: https://www.citrix.com/blogs/2020/01/22/citrix-and-fireeye-mandiant-share-forensic-tool-for-cve-2019-19781/

Additional FireEye Mandiant findings associated with CVE-2019-19781 can be found in the following blog post: https://www.fireeye.com/blog/products-and-services/2020/01/fireeye-and-citrix-tool-scans-for-iocs-related-to-vulnerability.html