As attacks begin, Citrix ships patch for VPN vulnerability

Igor Golovniov/SOPA Images/LightRocket via Getty Images

reader comments

22 with 20 posters participating

Share this story

On January 19, Citrix released some permanent fixes to a vulnerability on the company's Citrix Application Delivery Controller (ADC) and Citrix Gateway virtual private network servers that allowed an attacker to remotely execute code on the gateway without needing a login. The vulnerability affects tens of thousands of known VPN servers, including at least 260 VPN servers associated with US federal, state, and local government agencies—including at least one site operated by the US Army.

The patches are for versions 11.1 and 12.0 of the products, formerly marketed under the NetScaler name. Other patches will be available on January 24. These patches follow instructions for temporary fixes the company provided to deflect the crafted requests associated with the vulnerability, which could be used by an attacker to gain access to the networks protected by the VPNs.

Fermin J. Serna, chief information security officer at Citrix, announced the fixes in a blog post on Sunday. At the same time, Serna revealed that the vulnerability—and the patches

being released—also applied to Citrix ADC and Citrix Gateway Virtual Appliances hosted on virtual machines on all commercially available virtualization platforms, as well as those hosted in Azure, Amazon Web Services, Google Compute Platform, and Citrix Service Delivery Appliances (SDXs).

Lots to patch

That makes for lots of work over the next few weeks for Citrix customers, which include thousands of government agencies, educational institutions, hospitals, and major corporations worldwide.

As of last week, according to data provided by Bad Packets to Ars Technica, over 26,000 servers were still vulnerable to the crafted request. The data, including information on potentially vulnerable government VPN gateways, was shared by Bad Packets with the Cybersecurity and Infrastructure Security Agency. They included a gateway associated with a DOD civilian personnel system, the US Census service, and a number of local law enforcement agencies.

Inevitably, hundreds of Citrix VPN servers will remain vulnerable for weeks or months. Some are already being attacked, according to reports from FireEye—with one attacker installing the mitigation settings to keep other attackers out and booting any other installed malware before setting up their own backdoor.

Many of the exploits thus far have installed low-impact malware, including cryptocurrency mining software. But based on what happened with last year's Pulse Secure vulnerability, ransomware operators and other cybercriminals will soon join the hunt.

Meanwhile, a member of the group operating the REvil ransomware campaign recently acknowledged that the group had attacked Travelex using the Pulse Secure vulnerability,

according to security researcher Vitali Kremez. UNKN, the administrator of the REvil malware, claimed credit for the Travelex attack in a forum post on January 7 and said that Travelex executives needed to hurry up and pay, or customers' birth dates, Social Security numbers, and credit card data "would be sold to someone."

https://arstechnica.com/?p=1645999