'Friendly' hackers are seemingly fixing the Citrix server hole – and leaving a nasty present behind

By Shaun Nichols

Published: 2020-01-17 · Archived: 2026-04-05 12:51:55 UTC

Hackers exploiting the high-profile Citrix CVE-2019-19781 flaw to compromise VPN gateways are now patching the servers to keep others out.

Researchers at FireEye report finding a hacking group (dubbed NOTROBIN) that has been bundling mitigation code for NetScaler servers with its exploits. In effect, the hackers exploit the flaw to get access to the server, kill any existing malware, set up their own backdoor, then block off the vulnerable code from future exploit attempts by mitigation.

Obviously, this is less of a noble gesture and more of a way to keep others out of the pwned boxes.

"Upon gaining access to a vulnerable NetScaler device, this actor cleans up known malware and deploys NOTROBIN to block subsequent exploitation attempts," the FireEye team explained.

"But all is not as it seems, as NOTROBIN maintains backdoor access for those who know a secret passphrase. FireEye believes that this actor may be quietly collecting access to NetScaler devices for a subsequent campaign."

That the attackers would think to mitigate the bug is hardly surprising given the number of hackers believed to be scanning for and targeting the bug. It would make sense to take a compromised server off the map, so to speak, for other groups trying to exploit the so-called 'Shitrix' flaw.

FireEye says it has yet to work out all the details of the attack, but it is believed that most of the exploit is done through a single script. That script, delivered via an HTTP POST request, issues the commands to kill any cryptocurrency scripts running on the machine, creates a directory to stage the next phase of the attack, then downloads and runs the secondary NOTROBIN payload.

"Cryptocurrency miners are generally easy to identify—just look for the process utilizing nearly 100 per cent of the CPU," said FireEye. "By uninstalling these unwanted utilities, the actor may hope that administrators overlook an obvious compromise of their NetScaler devices."

Once the secondary payload has been downloaded and launched, it installs the backdoor for later access by the attackers, then proceeds to launch a pair of scripts that both search out and delete known malware on the machine and monitor and block any incoming attempts to exploit the vulnerability.

"The mitigation works by deleting staged exploit code found within NetScaler templates before it can be invoked," FireEye's team explained. "However, when the actor provides the hardcoded key during subsequent exploitation, NOTROBIN does not remove the payload. This lets the actor regain access to the vulnerable device at a later time."

While most vulnerable Citrix devices can be protected from attacks by applying the vendor's mitigations, some will need to update their firmware in order for the protections to actually work. Citrix has promised a complete patch for the flaw by January 20. ®
