

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

 theregister.co.uk/2020/01/17/hackers_patch_citrix_vulnerability/

Shaun Nichols

Security

Congratulations, you've won a secret backdoor

Shaun Nichols in San Francisco Fri 17 Jan 2020 // 19:49 UTC

9 

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.



Patch now: Published Citrix applications leave networks of 'potentially 80,000' firms at risk from attackers

READ MORE

"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. ®

Other stories you might like

- [Experts: AI should be recognized as inventors in patent law](#)

[Plus: Police release deepfake of murdered teen in cold case, and more](#)

[Katyanna Quach](#), Sat 28 May 2022 // 11:23 UTC **13** 

In-brief Governments around the world should pass intellectual property laws that grant rights to AI systems, two academics at the University of New South Wales in Australia argued.

Alexandra George, and Toby Walsh, professors of law and AI, respectively, believe failing to recognize machines as inventors could have long-lasting impacts on economies and societies.

"If courts and governments decide that AI-made inventions cannot be patented, the implications could be huge," they wrote in a comment article [published](#) in Nature.

"Funders and businesses would be less incentivized to pursue useful research using AI inventors when a return on their investment could be limited. Society could miss out on the development of worthwhile and life-saving inventions."

[Continue reading](#)

- [Declassified and released: More secret files on US govt's emergency doomsday powers](#)

[Nuke incoming? Quick break out the plans for rationing, censorship, property seizures, and more](#)

[Katyanna Quach](#), Sat 28 May 2022 // 08:51 UTC **26** 

More papers describing the orders and messages the US President can issue in the event of apocalyptic crises, such as a devastating nuclear attack, have been declassified and released for all to see.

These government files are part of a larger collection of records that discuss the nature, reach, and use of secret Presidential Emergency Action Documents: these are executive orders, announcements, and statements to Congress that are all ready to sign and send out as soon as a doomsday scenario occurs. PEADs are supposed to give America's commander-in-chief immediate extraordinary powers to overcome extraordinary events.

PEADs have never been declassified or revealed before. They remain hush-hush, and their exact details are not publicly known.

[Continue reading](#)

- [Stolen university credentials up for sale by Russian crooks, FBI warns](#)

[Forget dark-web souks, thousands of these are already being traded on public bazaars](#)

[Jessica Lyons Hardcastle](#) Fri 27 May 2022 // 22:34 UTC 

Russian crooks are selling network credentials and virtual private network access for a "multitude" of US universities and colleges on criminal marketplaces, according to the FBI.

According to a warning issued on Thursday, these stolen credentials sell for thousands of dollars on both dark web and public internet forums, and could lead to subsequent cyberattacks against individual employees or the schools themselves.

"The exposure of usernames and passwords can lead to brute force credential stuffing computer network attacks, whereby attackers attempt logins across various internet sites or exploit them for subsequent cyber attacks as criminal actors take advantage of users recycling the same credentials across multiple accounts, internet sites, and services," the Feds' alert [\[PDF\]](#) said.

[Continue reading](#)

- [Big Tech loves talking up privacy – while trying to kill privacy legislation](#)

[Study claims Amazon, Apple, Google, Meta, Microsoft work to derail data rules](#)

[Thomas Claburn in San Francisco](#) Fri 27 May 2022 // 21:48 UTC [7](#) 

Amazon, Apple, Google, Meta, and Microsoft often support privacy in public statements, but behind the scenes they've been working through some common organizations to weaken or kill privacy legislation in US states.

That's according to [a report](#) this week from news non-profit The Markup, which said the corporations hire lobbyists from the same few groups and law firms to defang or drown state privacy bills.

The report examined 31 states when state legislatures were considering privacy legislation and identified 445 lobbyists and lobbying firms working on behalf of Amazon, Apple, Google, Meta, and Microsoft, along with industry groups like TechNet and the State Privacy and Security Coalition.

[Continue reading](#)

- [SEC probes Musk for not properly disclosing Twitter stake](#)

[Meanwhile, social network's board rejects resignation of one its directors](#)

[Katyanna Quach](#) Fri 27 May 2022 // 21:26 UTC **11** 

America's financial watchdog is investigating whether Elon Musk adequately disclosed his purchase of Twitter shares last month, just as his bid to take over the social media company hangs in the balance.

A letter [[PDF](#)] from the SEC addressed to the tech billionaire said he "[did] not appear" to have filed the proper form detailing his 9.2 percent stake in Twitter "required 10 days from the date of acquisition," and asked him to provide more information. Musk's shares made him one of Twitter's largest shareholders. The letter is dated April 4, and was shared this week by the regulator.

Musk quickly moved to try and buy the whole company outright in a deal initially worth over \$44 billion. Musk sold a chunk of his shares in Tesla worth \$8.4 billion and bagged another \$7.14 billion from investors to help finance the \$21 billion he promised to put forward for the deal. The remaining \$25.5 billion bill was secured via debt financing by Morgan Stanley, Bank of America, Barclays, and others. But the takeover is not going smoothly.

[Continue reading](#)

- [Cloud security unicorn cuts 20% of staff after raising \\$1.3b](#)

[Time to play blame bingo: Markets? Profits? Too much growth? Russia? Space aliens?](#)

[Jessica Lyons Hardcastle](#) Fri 27 May 2022 // 19:19 UTC **14** 

Cloud security company Lacework has laid off 20 percent of its employees, just months after two record-breaking funding rounds pushed its valuation to \$8.3 billion.

A spokesperson wouldn't confirm the total number of employees affected, though told *The Register* that the "widely speculated number on Twitter is a significant overestimate."

The company, as of March, counted more than 1,000 employees, which would push the jobs lost above 200. And the widely reported number on Twitter is about 300 employees. The biz, based in Silicon Valley, was founded in 2015.

[Continue reading](#)

- [Talos names eight deadly sins in widely used industrial software](#)

[Entire swaths of gear relies on vulnerability-laden Open Automation Software \(OAS\)](#)

[Jeff Burt](#) Fri 27 May 2022 // 18:30 UTC **2** 

A researcher at Cisco's Talos threat intelligence team found eight vulnerabilities in the Open Automation Software (OAS) platform that, if exploited, could enable a bad actor to access a device and run code on a targeted system.


The OAS platform is widely used by a range of industrial enterprises, essentially facilitating the transfer of data within an IT environment between hardware and software and playing a central role in organizations' industrial Internet of Things (IIoT) efforts. It touches a range of devices, including PLCs and OPCs and IoT devices, as well as custom applications and APIs, databases and edge systems.

Companies like Volvo, General Dynamics, JBT Aerotech and wind-turbine maker AES are among the users of the OAS platform.

[Continue reading](#)

- [Despite global uncertainty, \\$500m hit doesn't rattle Nvidia execs](#)

[CEO acknowledges impact of war, pandemic but says fundamentals 'are really good'](#)

[Dylan Martin](#) Fri 27 May 2022 // 16:08 UTC **1** 

Nvidia is expecting a \$500 million hit to its global datacenter and consumer business in the second quarter due to COVID lockdowns in China and Russia's invasion of Ukraine. Despite those and other macroeconomic concerns, executives are still optimistic about future prospects.


"The full impact and duration of the war in Ukraine and COVID lockdowns in China is difficult to predict. However, the impact of our technology and our market opportunities remain unchanged," said Jensen Huang, Nvidia's CEO and co-founder, during the company's first-quarter earnings call.

Those two statements might sound a little contradictory, including to some investors, particularly following the [stock selloff](#) yesterday after concerns over Russia and China prompted Nvidia to issue lower-than-expected guidance for second-quarter revenue.

[Continue reading](#)

- [Another AI supercomputer from HPE: Champollion lands in France](#)

[That's the second in a week following similar system in Munich also aimed at researchers](#)

[Dan Robinson](#) Fri 27 May 2022 // 15:30 UTC 2 

HPE is lifting the lid on a new AI supercomputer – the second this week – aimed at building and training larger machine learning models to underpin research.

Based at HPE's Center of Excellence in Grenoble, France, the new supercomputer is to be named Champollion after the French scholar who made advances in deciphering Egyptian hieroglyphs in the 19th century. It was built in partnership with Nvidia using AMD-based Apollo computer nodes fitted with Nvidia's A100 GPUs.

Champollion brings together HPC and purpose-built AI technologies to train machine learning models at scale and unlock results faster, HPE said. HPE already provides HPC and AI resources from its Grenoble facilities for customers, and the broader research community to access, and said it plans to provide access to Champollion for scientists and engineers globally to accelerate testing of their AI models and research.

[Continue reading](#)

- [Workday nearly doubles losses as waves of deals pushed back](#)

[Figures disappoint analysts as SaaS HR and finance application vendor navigates economic uncertainty](#)

[Lindsay Clark](#) Fri 27 May 2022 // 14:30 UTC 9 

HR and finance application vendor Workday's CEO, Aneel Bhusri, confirmed deal wins expected for the three-month period ending April 30 were being pushed back until later in 2022.

The SaaS company boss was speaking as Workday recorded an operating loss of \$72.8 million in its first quarter [[PDF](#)] of fiscal '23, nearly double the \$38.3 million loss recorded for the same period a year earlier. Workday also saw revenue increase to \$1.43 billion in the period, up 22 percent year-on-year.

However, the company increased its revenue guidance for the full financial year. It said revenues would be between \$5.537 billion and \$5.557 billion, an increase of 22 percent on earlier estimates.

[Continue reading](#)

- [UK monopoly watchdog investigates Google's online advertising business](#)

[Another probe? Mountain View is starting to look like a pincushion at this rate](#)

[Richard Currie](#) Fri 27 May 2022 // 14:00 UTC 6 

The UK's Competition and Markets Authority is lining up yet another investigation into Google over its dominance of the digital advertising market.

This latest inquiry, [announced Thursday](#), is the second major UK antitrust investigation into Google this year alone. In March this year the UK, together with the European Union, said it wished to examine Google's ["Jedi Blue" agreement](#) with Meta to allegedly favor the former's Open Bidding ads platform.

The news also follows [proposals](#) last week by a bipartisan group of US lawmakers to create legislation that could force Alphabet's Google, Meta's Facebook, and Amazon to divest portions of their ad businesses.

[Continue reading](#)