idea LOGICAL

LOGICAL TALK · AUGUST-SEPTEMBER 2021

A Vulnerability Exploited: Fortigate SSL-VPN Credentials Leak Incident

The security landscape around the world is constantly evolving and maintaining all systems—especially security devices—is essential in staying ahead of cybercriminals. One of the most prime targets for threat actors are the technology vendors and Fortinet – the cybersecurity solution provider is no exception.

What happened with Fortinet in 2019?

In August 2019, Fortinet announced the detection for two of their SSL VPN vulnerabilities – CVE-2018-13379 (FG-IR-18-384) and CVE-2018-13383 (FG-IR-18-388).

CVE-2018-13379 (FG-IR-18-384) – This path traversal vulnerability in the FortiOS SSL VPN web portal could've potentially allowed an unauthenticated attacker to download files through specially crafted HTTP resource requests.

CVE-2018-13383 (FG-IR-18-388) – This heap buffer overflow vulnerability in the FortiOS SSL VPN web portal had the potential to cause the SSL VPN web service for logged-in users. It could also potentially allow remote code execution on FortiOS due to a failure to handle JavaScript href content properly. This would require an authenticated user to visit a specifically crafted and proxied webpage.

Both the vulnerabilities could lead to severe data leaks if the released patch were not applied. "We urge customers to immediately implement all appropriate patch updates and signatures, with a firmware upgrade still the primary recommended solution," remedy mentioned by the FortiGuard Labs.

What is happening with Fortinet in 2021?

Fast forward to June 2021, FBI announced that threat actors have gained access to a local U.S. municipal government network. This breach was executed by exploiting vulnerabilities in an unpatched Fortinet networking appliance.

With no surprises to the security experts, it has been quickly discovered that the breach was not a result of a new attack but slow exploitation of the 2019 vulnerability.

The FBI announcement resulted in evidence proving that there are still unpatched devices in the wild being actively targeted by criminal organizations. This further highlights the risk of organizations choosing to abstain from vendor, industry, and governmental advice by not proactively updating their devices or not following password change instructions.

Join Us For Our Next LIVE Session Later This Month

Cybersecurity has been a priority for PROACTIVE Canadian business leaders for many years. How do you know if you have made the right choices to prepare your business for complex and evolving cyberattacks?
Join our president – Andre Vittorio, in an open conversation with Toronto Police Services and Cyber Insurance Expert on Tuesday, Sept 28 at 2 p.m.
Register Here

Is it possible to avoid a cyber incident or a cyber breach after a vulnerability is discovered?

Absolutely! If a vulnerability is discovered and made public in time, a cyber incident or a cyber breach is avoidable by following the guidelines given by the vendor, who in this case is Fortinet. "This and similar incidents highlight that the failure to patch vulnerable systems still represents one of the most critical security gaps in many organizations and is responsible for the vast majority of network breaches and data loss," mentioned in the most recent blog by Fortinet.

Learn the difference between a cyber incident and a cyber breach.

How is Idealogical working on this Fortinet issue?

"Idealogical has been proactively updating the patches released since 2019. Additionally, our plan to update and deploy the most recent patches released by Fortinet is rolling out this week (the week of Sept 13, 2021).

Once the patches are deployed, we will reach out to each of our clients with details on what action should be taken from their end. For example, a password reset", says Andre de Lacerda, Technical Manager, Idealogical Systems Inc.

Back To School 2021 – Cybersecurity Tips for Parents and Students

After a long gap of almost 17 months, children are back to school this fall in most cities across the Greater Toronto Area. As great as in-person learning is, it comes with its own invisible detriments when it comes to the cybersecurity of the children.
In the digital age of multiple screens and new social media platforms, it can be challenging for parents to keep up with their kid's internet activities.

Quick Cybersecurity Tips for Parents

- Instill good cyber hygiene practices in your children by encouraging them to use different passwords for different accounts.
- Give them access to a password management tool like LastPass, so they don't have to worry about remembering every password they have ever created.
- Wherever possible, activate two-factor authentication on their devices and different online apps that they use. Read this article on how to activate 2FA on your favourite mobile apps.
- Recognize that your children are tech-savvy but not cyber-savvy. So, get involved by learning about their devices and platforms, mainly how to configure parental controls and privacy settings.
- Educate them on how to differentiate a legitimate email from a scam email. Read this quick guide on how to practice good email hygiene for cybersecurity.

Recognize that your children are tech-savvy but not cyber-savvy.

Quick Cybersecurity Tips for Students

- Avoid keeping your laptops, iPad, and phones unattended at school even when you are with your most trusted friends.
- Ensure your devices and all the apps and software on those devices are up to date.
- Sign-up for auto-update for software whenever possible.
- Ensure that you have screen locks for all your devices and that you lock your devices when not in use (do this even when the device is right in front of you). Threat actors can access unlocked devices from their remote locations.
- Educate yourself on phishing scams. Watch this video to learn about how different phishing attacks are executed.

Superstar Of The Month

Luv Bakshi

At Idealogical, we are a group of professionals who are always ready to help each other and push our peers to succeed in their roles. Every week we all take time to let our peers know how much we appreciate them by giving them "praise." Each of us have three praises to give every week. The team member who has the highest praises for the month is recognized as our Superstar of the Month. Join us in congratulating Luv Bakshi as our Superstar of the month for July and Guilherme Siqueira for August 2021.

Guilherme Siqueira