JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA21-092A

April 2, 2021

APT Actors Exploit Vulnerabilities to Gain Initial Access for Future Attacks

SUMMARY

In March 2021 the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) observed Advanced Persistent Threat (APT) actors scanning devices on ports 4443, 8443, and 10443 for CVE-2018-13379, and enumerated devices for CVE-2020-12812 and CVE-2019-5591. It is likely that the APT actors are scanning for these vulnerabilities to gain access to multiple government, commercial, and technology services networks. APT actors have historically exploited critical vulnerabilities to conduct distributed denial-of-service (DDoS) attacks, ransomware attacks, structured query language (SQL) injection attacks, spearphishing campaigns, website defacements, and disinformation campaigns.

TECHNICAL DETAILS

The FBI and CISA have information indicating APT actors are using multiple CVEs to exploit Fortinet FortiOS vulnerabilities. The FBI and CISA believe the APT actors are likely exploiting these Fortinet FortiOS vulnerabilities—CVE 2018-13379, CVE-2020-12812, and CVE-2019-5591—to gain access to multiple government, commercial, and technology services networks.

The APT actors may be using any or all of these CVEs to gain access to networks across multiple critical infrastructure sectors to gain access to key networks as pre-positioning for follow-on data exfiltration or data encryption attacks. APT actors may use other CVEs or common exploitation techniques—such as spearphishing—to gain access to critical infrastructure networks to pre-position for follow-on attacks.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact..

Disclaimer: *The information in this Joint Cybersecurity Advisory is provided "as is" for informational purposes only. FBI and CISA do not provide any warranties of any kind regarding this information or endorse any commercial product or service, including any subjects of analysis.*

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp/.

MITIGATIONS

Organizations should take the following:

- Immediately patch CVEs 2018-13379, 2020-12812, and 2019-5591.
- If FortiOS is not used by your organization, add key artifact files used by FortiOS to your organization's execution deny list. Any attempts to install or run this program and its associated files should be prevented.
- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the primary system where the data resides.
- Implement network segmentation.
- Require administrator credentials to install software.
- Implement a recovery plan to restore sensitive or proprietary data from a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Use multifactor authentication where possible.
- Regularly change passwords to network systems and accounts, and avoid reusing passwords for different accounts. Implement the shortest acceptable timeframe for password changes.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update antivirus and anti-malware software on all hosts.
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.
- Focus on awareness and training. Provide users with training on information security principles and techniques, particularly on recognizing and avoiding phishing emails.

CONTACT INFORMATION

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat.

For any questions related to this report or to report an intrusion and request resources for incident response or technical assistance, please contact:

- The FBI through the FBI Cyber Division or a local field office,
- CISA