THREAT BULLETINS

APT Actors Exploiting Fortinet Vulnerabilities to Gain Access for Malicious Activity

TLP:WHITE

May 27, 2021

The United States Federal Bureau of Investigation (FBI) is continuing to warn about Advanced Persistent Threat (APT) actors exploiting Fortinet vulnerabilities. As of at least May 2021, an APT actor group almost certainly exploited a Fortigate appliance to access a webserver hosting the domain for a U.S. municipal government. The APT actors likely created an account with the username “elie” to further enable malicious activity on the network.

The FBI and the Cybersecurity and Infrastructure Security Agency (CISA) previously warned in April 2021 that APT actors had gained access to devices on ports 4443, 8443, and 10443 for Fortinet FortiOS CVE-2018-13379, and

enumerated devices for FortiOS CVE-2020-12812 and FortiOS CVE-2019-5591. Access gained by the APT actors can be leveraged to conduct data exfiltration, data encryption,or other malicious activity. The APT actors are actively targeting a broad range of victims across multiple sectors, indicating the activity is focused on exploiting vulnerabilities rather than targeted at specific sectors. Please see Joint Cybersecurity Advisory AA21-092A, published 2 April 2021, for more information on this activity.

The APT actors may have established new user accounts on domain controllers, servers, workstations, and the active directories. Some of these accounts appear to have been created to look similar to other existing accounts on the network, so specific account names may vary per organization. In addition to unrecognized user accounts or accounts established to masquerade as existing accounts, the following account usernames may be associated with this activity:

- “elie”
- “WADGUtilityAccount”

Indicators of Compromise:

The FBI identified the following indicators of compromise (IOCs) that we assess are likely associated with this APT activity.

frpc.exe:

- MD5: b90f05b5e705e0b0cb47f51b985f84db
- SHA-1: 5bd0690247dc1e446916800af169270f100d089b
- SHA-256: 28332bdbfaeb8333dad5ada3c10819a1a015db9106d5e8a74beaaf03797511aa

Frps.exe:

- MD5: 26f330dadcdd717ef575aa5bfcdbe76a
- SHA-1: c4160aa55d092cf916a98f3b3ee8b940f2755053

- SHA-256: d7982ffe09f947e5b4237c9477af73a034114af03968e3c4ce462a029f072a5a

Associated Tools:

- Mimikatz (credential theft)
- MinerGate (crypto mining)
- WinPEAS (privilege escalation)
- SharpWMI (Windows Management Instrumentation)
- BitLocker activation when not anticipated (data encryption)
- WinRARwhere not expected(archiving)
- FileZilla where not expected (file transfer)

Report Source(s)	FBI

Recommendations

- Immediately patch CVEs 2018-13379, 2020-12812, and 2019-5591.
- If FortiOS is not used by your organization, add the key artifact files used by FortiOS to your organization's execution deny list. Any attempts to install or run this program and its associatedfiles should be prevented.
- Review domain controllers, servers, workstations,and active directories for new or unrecognized user accounts.
- Review Task Scheduler for unrecognized scheduled tasks. Additionally, manually review operating system defined or recognized scheduled tasks for unrecognized "actions" (for example: review the steps each scheduled task is expected to perform).
- Review antivirus logs for indications they were unexpectedly turned off.
- 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 system where the data resides.
- Implement network segmentation.

- Require administrator credentials to install software.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in 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 time frame 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.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a virtual private network (VPN).
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.

Sources
Actors Exploit Fortinet.pdf (MI-000148-MW)

See Attached

Alert ID b2b7c0de

View Alert

Tags APT Actors, FBI Flash, Fortinet

For Questions or Comments Please email us at toc@h-isac.org

FBI The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts may be identified

at www.fbi.gov/contact-us/field. Contact CyWatch by telephone at 855-292-3937 or by email at CyWatch@fbi.gov.

Download Health-ISAC's Information Sharing App. 

For more update and alerts, visit: **https://health-isac.cyware.com**