National Cyber Security Centre
a part of GCHQ

Alert: Critical risk to unpatched Fortinet VPN devices from continuing exploitation of CVE-2018-13379

Version 2.0

8 April 2021

April 2021 update

APT actors are still actively scanning for CVE-2018-13379 and attempting to exploit it. The NCSC is aware of such activity continuing in 2021.

In April CISA and the FBI also published an advisory on Fortinet vulnerabilities. In addition to CVE-2018-13379, they have evidence that APTs are actively scanning for and exploiting two other Fortinet vulnerabilities CVE-2020-12812 and CVE-2019-5591. The NCSC advises organisations to also ensure they have patched these two vulnerabilities as well as CVE-2018-13379.

For information and links to updates, please see the CISA/FBI report.

*The NCSC's advice to organisations remains to ensure the latest security updates are installed as soon as is practicable for **all** vulnerabilities.*

Introduction

The NCSC is concerned that a significant number of organisations in the UK have not patched the Fortinet VPN vulnerability CVE-2018-13379. This continues to be actively exploited by Advanced Persistent Threat groups (APTs) and cyber criminals.

This follows information in late November 2020 that credentials for 50,000 vulnerable Fortinet VPNs worldwide were stolen and then published in a hacker forum.

This alert provides more detail and recommends actions for organisations using affected products.

Details

In May 2019 Fortinet disclosed and provided a security update for a path traversal vulnerability in Fortinet devices running SSL VPN with local authentication for users. The following versions are affected:

FortiOS 6.0 - 6.0.0 to 6.0.4

FortiOS 5.6 - 5.6.3 to 5.6.7

FortiOS 5.4 - 5.4.6 to 5.4.12

The NCSC later reported in 2019 that APTs were exploiting this vulnerability along with other vulnerabilities affecting other VPN products where updates were not installed. Cyber criminals and APT actors are continuing to exploit this unpatched vulnerability in 2020 and the NCSC has observed an increase in attempts to exploit it since publication of the credentials.

UK impact

In addition to credentials, hackers have also stolen and published the session IPs relating to the unpatched devices. **Over 600 of these IPs are located in the UK**, meaning that a significant number of UK devices are at very high risk of exploitation.

The NCSC is advising organisations which are using Fortinet VPN devices where security updates have not been installed, **to assume they are now compromised and to begin incident management procedures.**

Fortinet has also sent tailored email notifications to users running the impacted versions but the NCSC recommends that action is taken even if an organisation has not received an email notification.

Advice for users

Users of all Fortinet VPN devices should check whether the 2019 updates have been installed. If not, the NCSC recommends that as soon as possible, the affected device should be removed from service, returned to a factory default, reconfigured and then returned to service.

During incident investigation, organisations should investigate all connected hosts and networks to identify any further attacker movement and activities. Anomalous connections in access logs for the SSL VPN service may also indicate use of compromised credentials.

Organisations should then make it a high priority to upgrade to the latest FortiOS versions to prevent reinfection.

Additional measures

CERT New Zealand has highlighted that organisations may be able to confirm compromise by checking Fortinet device logs. This advice will help identify if the Metasploit payload[1] has been used, although organisations should note actors may have since modified behaviour and a nil return does not indicate that exploitation has not occurred.

Fortinet is also making efforts to help users mitigate this vulnerability and engaging in proactive security.

[1] The Metasploit payload can be found here: https://www.exploit-db.com/exploits/47287

Conclusion

This recent activity emphasises the importance of NCSC advice to install security updates as soon as is practicable following their release to ensure action is taken before exploitation is observed.

UK organisations should report any incidents to the NCSC via our website.

Mitigation

A variety of mitigations will be useful in defending against the campaigns detailed in this report:

- **Update your systems and software.** Ensure your operating system and productivity apps are up to date. Users with Office 365 licensing can use 'click to run' to keep their office applications seamlessly updated. See NCSC Guidance: https://www.ncsc.gov.uk/collection/mobile-device-guidance/keeping-devices-and-software-up-to-date
- **Review and refresh your incident management processes.** See NCSC Guidance: https://www.ncsc.gov.uk/collection/incident-management
- **Prevent and detect lateral movement in your organisation's networks**. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/preventing-lateral-movement.
- **Set up a security monitoring capability** so you are collecting the data that will be needed to analyse network intrusions. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes and https://www.ncsc.gov.uk/information/logging-made-easy
- **Further information:** Invest in preventing malware-based attacks across various scenarios. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks