UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0326

FORTINET PATCHES CRITICAL RCE FLAW

DATE ISSUED: 15th June 2023

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

Fortinet has released security updates that fix an undisclosed, critical pre-authentication Remote Code Execution (RCE) vulnerability in FortiOS firmware versions. It could allow an unauthorised agent to execute remote code without requiring the attacker to log in to exploit it.

BREAKDOWN

Fortinet has released several versions of FortiOS, the operating system/firmware powering its Fortigate firewalls and other devices. Lexfo security researcher Charles Fol reported that the new FortiOS updates include a fix for a critical RCE vulnerability tracked as CVE-2023-27997 that could allow unauthorised agents to interfere via the VPN, even if the MFA is enabled. Fortinet has yet to publish an advisory. However, Fortinet pushed the security fixes on Friday in FortiOS firmware versions 7.0.12, 7.2.5, 6.4.13, 6.2.15, and v6.0.17 (Fortinet officially stopped supporting the 6.0 branch last year). This should be considered an urgent patch for Fortinet admins as threat actors will quickly analyse and discover it. Vulnerabilities affecting Fortigate firewalls have been a popular target in the past. Also, Fortinet has been known to push out critical fixes without mentioning vulnerabilities – whether actively exploited or not. It is recommended that Enterprise admins implement the security patches as soon as possible.

REMEDIATION STEPS

- Apply the Fortinet security updates as soon as possible.
- Update all credentials related to the affected appliances.
- Use network traffic monitoring tools to identify unusual traffic and behaviour patterns that may indicate malware activity

REFERENCES & RESOURCES

Bleeping Computer	https://www.bleepingcomputer.com/news/security/fortinet-fixes-critical-rce-flaw-in-fortigate-ssl-vpn-devices-patch-now/
Twitter	https://twitter.com/cfreal_/status/1667852157536616451
Cert NZ	https://www.cert.govt.nz/it-specialists/advisories/fortigate-ssl-vpn-remote-code-execution-vulnerability/