U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00188

FORTINET BUG ALLOWS FIREWALL TAKEOVER

DATE ISSUED: 23rd August 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

An Operating System (OS) command-injection vulnerability present in Fortinet's Web Application Firewall (WAF) FortiWeb – if unpatched, could mean attackers are able to elevate privileges and gain full device control.

BREAKDOWN

Using backticks and the 'Name" field of the SAML Server configuration page, an authenticated attacker who has access to the FortiWeb management interface would be able to introduce commands into the OS and do whatever they please. This may include lateral movement across an environment beyond the Demilitarized Zone (DMZ) deeper into the company's infrastructure, establish an Advanced Persistent Threats, add malicious shells, install cryptominers and other malware and much more. Although an attacker must be logged in to the platform to conduct the attack, it may be daisy-chained with another vulnerability to gain access CVE-2020-29015. Affected versions include 6.3.1 and prior.

REMEDIATION STEPS

- Check for updates set to be released by Fortinet at the end of August
- Ensure access to the FortiWeb is not exposed directly to the internet and may only be reached by trusted internal networks.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/unpatched-fortinet-bug-firewall-takeovers/168764/
ZDNet	https://www.zdnet.com/article/fortinet-slams-rapid7-for-disclosing-vulnerability-before-end-of-90-day-window
Rapid7	https://www.rapid7.com/blog/post/2021/08/17/fortinet-fortiweb-os-command-injection/