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

CYBER GUIDANCE ISSUE 0279

FORTINET FIXES CRITICAL RCE VULNERABILTIES

DATE ISSUED: 20th February 2023

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

OVERVIEW

The cybersecurity solutions firm Fortinet has addressed two critical-severity vulnerabilities in its products which could allow arbitrary code execution. This vulnerability could allow an attacker to run any commands or code on a target machine via specifically crafted HTTP request without the owner's knowledge.

BREAKDOWN

Fortinet has released security updates to address ciritical vulnerabilties for its FortiNAC and FortiWeb products. The first security flaw impacts FortiNAC which is a network access control solution that provides protection against threat by continuously monitoring the network. The vulnerability in FortiNAC is tracked as CVE-2022-39952 and has a CVSS score of 9.8. The affected ForitNAC versions 9.4.0, 9.2.0 through 9.2.5, 9.1.0 through 9.1.7, all 8.8 versions, all 8.7 versions, all 8.6 versions , all 8.5 versions, and all 8.3 versions. The second critical vulnerability with a CVSS score of 9.3 is tracked as CVE-2021-42756, a multiple stack-based buffer overflow vulnerability in the proxy daemon and affects FortiWeb 5.x all versions, 6.0.7 and below, 6.1.2 and below, 6.2.6 and below, 6.3.16 and below, 6.4 all versions.

REMEDIATION STEPS

- Update and patch the systems to the latest versions.
- Schedule regular malware and vulnerability scans. It provides an opportunity to mitigate potential security flaws at an early stage.
- Check network device security, access control permissions and open ports and monitor for abnormal activity.
- Implement security-in-depth/defense-in-depth multilayered protections

REFERENCES & RESOURCES

The Bleeping Computer https://www.bleepingcomputer.com/news/security/fortinet-fixes-critical-rce-flaws-in-fortinac-and-fortiweb/