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

CYBER GUIDANCE ISSUE 0332

FORTINET PATCHES CRITICAL RCE FLAW

DATE ISSUED: 28th June 2023

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

OVERVIEW

The cybersecurity solutions firm Fortinet has fixed multiple vulnerabilities in its FortiNAC solution. The most critical-severity vulnerability could allow an attacker to perform arbitrary code execution. It could allow attackers to install programs, view, change or delete data, and create new accounts with administrative privileges.

BREAKDOWN

FortiNAC is a zero-trust access solution that oversees and protects all digital assets connected to the enterprise network. It allows organisations to manage network access policies and secure the network from unauthorised access and threats. Multiple vulnerabilities have been discovered in the FortiNAC solution, the most severe of which is tracked as CVE-2023-33299, with a CVSS score of 9.6. It is a deserialisation of untrusted data vulnerability that could allow an unauthenticated attacker to execute unauthorised code or commands via malicious requests sent to the service on TCP port 1050. The products impacted by this are FortiNAC versions below 7.2.1, below 9.4.3, below 9.2.8 and all earlier versions of 8. x. Due to the network's level of access and control, various malicious actors have targeted Fortinet devices, exploiting zero-day vulnerabilities and attacking organisations that have failed to apply necessary patches and updates.

REMEDIATION STEPS

- Apply the necessary updates provided by Fortinet.
- Implement an automated patch management solution to regularly perform operating system and application updates on enterprise assets.
- Exercise identifying, assessing, and mitigating vulnerabilities in computer systems, networks, and applications via a vulnerability management process.
- Practice the Principle of Least Privilege on all systems and services to lower the risk of attacks.

REFERENCES & RESOURCES

CIS Advisories https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-fortinet-fortinac-could-allow-for-arbitrary-code-execution_2023-068

Bleeping Computer https://www.bleepingcomputer.com/news/security/fortinet-fixes-critical-fortinac-remote-command-execution-flaw/