U UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 0283

EXPLOIT GUIDE RELEASED FOR FORTINET RCE BUG

DATE ISSUED: 27th February 2023

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

OVERVIEW

Security researches at Horizon3 released a technical post detailing how to exploit a critical Remote Code Execution (RCE) flaw in Fortinet's FortiNAC network access control suite. The vulnerbailty could allow an attacker to execute arbitrary code on a remote device and gain privilidge access on the system.

BREAKDOWN

Fortinet recently revealed and patched a critical RCE vulnerability in its FortiNAC product. The vulnerability is tracked as CVE-2022-39952 and has a rating of 9.8 on the CVSS vulnerability-severity scale. It could allow an unauthenticated attacker to write arbitrary files on the system and execute arbitrary code as a root user. Researches at Horizon3 released a blog post with technical analysis and a proof-of-concept exploit for this vulnerability. The exploit code is also released on the company's repository on Github which could be leveraged both by an attacker to automate the process or a defender to create valid protection measures. FortiNAC 9.4.0, 9.2.0 through 9.2.5, 9.1.0 through 9.1.7, and all versions on the 8.8, 8.7, 8.6, 8.5, and 8.3 are advised to be update urgently.

REMEDIATION STEPS

- Update and patch the FortiNAC products to the latest versions.
- Deploy network security solutions that can block attempted exploitation of vulnerable applications and that can detect any anomalous behaviour.
- Implementing network segmentation, access management, and adopt a security strategy based on zero-trust principles. An organization can limit an attacker's ability to move through the network and take advantage of their initial access to corporate systems.

REFERENCES & RESOURCES

The Bleeping Computer https://www.bleepingcomputer.com/news/security/exploit-released-for-critical-fortinet-rce-flaw-patch-now/