Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3: Sector Alert

November 21, 2023 TLP:CLEAR Report: 202311211500

Critical Vulnerability in Fortinet FortiSIEM Platform

Executive Summary

Fortinet has identified a vulnerability in its FortiSIEM platform, which is utilized by the Healthcare and Public Health (HPH) sector. This vulnerability enables a threat actor to execute commands on the target system, allowing for a potentially wide-scale and impactful cyberattack. HC3 recommends that all healthcare organizations operating FortiSIEM prioritize the upgrade of these platforms in a timely manner.

Report

On November 14th, the cybersecurity company Fortinet released an alert for an OS command injection vulnerability in versions 4.7 through 5.4 of their FortiSIEM platform. Fortinet describes this system as a unified event correlation and risk management platform that uses machine learning to detect unusual user and entity behavior without requiring the administrator to write complex rules. This platform is used in the HPH sector, as it has capabilities tailored for health-related applications. This vulnerability is tracked as CVE-2023-36553 (and tracked as FG-IR-23-135 by Fortinet) and if exploited, it can allow a remote, unauthenticated attacker to use crafted API requests to execute unauthorized code or commands. As of the release of this report, this vulnerability is not known to be actively exploited in the wild. However, this is subject to change at any time.

Patches, Mitigations, and Workarounds

There are no known mitigations or workarounds. In order to patch this vulnerability, the FortiSIEM platform must be upgraded in accordance with the instructions in the alert. HC3 recommends that all healthcare organizations operating FortiSIEM prioritize the upgrade of these platforms in a timely manner.

References

Fortinet PSIRT: FG-IR-23-135
https://www.fortiguard.com/psirt/FG-IR-23-135

Fortinet warns of critical command injection bug in FortiSIEM
https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-command-injection-bug-in-fortisiem/

MITRE CVE-2023-36553
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2023-36553

NISA CVE-2023-36553 Detail
https://nvd.nist.gov/vuln/detail/CVE-2023-36553

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback