KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Hackers exploiting Fortinet's critical auth bypass vulnerability

Tracker ID: TN1009 **Date:** 11/Oct/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Background

Fortinet has issued a security warning to its customers regarding a flaw in FortiOS, FortiProxy web proxies and FortiSwitchManager that could allow an attacker to perform unauthorized actions on susceptible systems. CVE-2022-40684 (CVSS score: 9.6) is a critical issue that relates to an authentication bypass vulnerability that may allow an unauthenticated attacker to perform arbitrary activities on the administrative interface via a well-designed HTTP(S) request.

They have advised some of their clients via email that remote management user interfaces on impacted equipment should be turned off immediately. There is a known instance of this vulnerability being exploited. Thus, it is strongly recommended to verify the systems for the following indicators of compromise in the device logs: user="Local Process Access".

Administrators can block incoming attacks by deactivating HTTP/HTTPS administrative interfaces or using a Local in Policy to limit the IP addresses that can access the administrative interface. As a result, remote attackers will be unable to bypass authentication and log into vulnerable devices. The Fortinet PSIRT advisory includes thorough instructions for disabling the vulnerable admin interface for FortiOS, FortiProxy, and FortiSwitchManager, as well as restricting access by IP address.

Analysis

CVE ID	Severity	CVSS Score
CVE-2022-40684	Critical	9.6

Affected Products and Versions

- FortiOS version 7.2.0 through 7.2.1
- FortiOS version 7.0.0 through 7.0.6
- FortiProxy version 7.2.0
- FortiProxy version 7.0.0 through 7.0.6
- FortiSwitchManager version 7.2.0
- FortiSwitchManager version 7.0.0

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Hackers exploiting Fortinet's critical auth bypass vulnerability

Tracker ID: TN1009 **Date:** 11/Oct/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Recommendations

- Fortinet has released the security patches. Update FortiOS to version 7.0.7 or above and 7.2.2 or above; FortiProxy to version 7.0.7 or above and 7.2.1 or above, and FortiSwitchManager to version 7.2.2 or above.
- It is also recommended to immediately validate your systems against the following indicator of compromise in the device's logs: user="Local_Process_Access"
- Follow the workarounds shared by Fortinet in case updates are being delayed.
- Monitor the services and critical assets exposed to the Internet.
- Collect and review relevant logs, data, and artifacts to identify any threat in the network.

References

- Fortinet, FortiOS / FortiProxy - Authentication bypass on administrative interface, PSIRT Advisories, 10th October 2022, External Link (www.fortiguard.com).
- Ravie Lakshmanan, Fortinet Warns of Active Exploitation of Newly Discovered Critical Auth Bypass Bug, The Hacker News, 11th October 2022, External Link (thehackernews.com).
- Ravie Lakshmanan, Fortinet Warns of New Auth Bypass Flaw Affecting FortiGate and FortiProxy, The Hacker News, 7th October 2022, External Link (thehackernews.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia