Fortinet Releases Security Advisories for FortiOS

Date: 09th February 2024 | Severity: High

Summary

Fortinet released security updates to address critical remote code execution vulnerabilities in FortiOS (CVE-2024-21762, CVE-2024-23313). A cyber threat actor could exploit these vulnerabilities to take control of an affected system.

Attack Vectors

Fortinet is warning that a new critical remote code execution vulnerability in FortiOS SSL VPN is potentially being exploited in attacks. The flaw (tracked as CVE-2024-21762 / FG-IR-24-015) received a 9.6 severity rating and is an out-of-bounds write vulnerability in FortiOS that allows unauthenticated attackers to gain remote code execution (RCE) via maliciously crafted requests.

Fortinet disclosed that Chinese state-sponsored threat actors known as Volt Typhoon targeted FortiOS vulnerabilities to deploy custom malware known as COATHANGER. This malware is a custom remote access trojan (RAT) designed to infect FortiGate network security appliances and was recently found used in attacks on the Dutch Ministry of Defence. Due to the high severity of the newly disclosed CVE-2024-21762 flaw and the likelihood of it being exploited in attacks, it is strongly advised that you update your devices as soon as possible.

Indicator of Compromise

INDICATOR TYPE	INDICATORS
File Hash	NA

Recommendation

To patch the bug, Fortinet recommends upgrading to one of the latest versions based on this table:

Version	Affected	Solution
FortiOS 7.6	Not affected	Not Applicable
FortiOS 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above
FortiOS 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above
FortiOS 7.0	7.0.0 through 7.0.13	Upgrade to 7.0.14 or above
FortiOS 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above
FortiOS 6.2	6.2.0 through 6.2.15	Upgrade to 6.2.16 or above
FortiOS 6.0	6.0 all versions	Migrate to a fixed release

Reference Links

https://www.bleepingcomputer.com/news/security/new-fortinet-rce-flaw-in-ssl-vpn-likely-exploited-in-attacks/

exploited-in-attacks/https://www.cisa.gov/news-events/alerts/2024/02/09/fortinet-releases-security-advisories-fortios