Fortinet FortiOS, FortiSIEM Critical-Security Vulnerabilities

In February 2024, Fortinet disclosed two critical security flaws regarding FortiOS, the operating system used by Fortigate SSL VPNs, and FortiProxy. The Cybersecurity and Infrastructure Security Agency (CISA) added the two vulnerabilities as CVE-2024-21762, a format string vulnerability, and CVE-2024-23113, an out-of-bounds write vulnerability, both with a CVSS score of 9.8. These vulnerabilities allow attackers to bypass authentication and execute arbitrary commands or code through exposed Fortinet SSL VPNs through specially crafted HTTP requests. Fortinet also disclosed two additional critical flaws for FortiSIEM, documented as CVE-2024-23108 and CVE-2024-23109, both which also received a CVSS score of 9.8 and allow for OS command injections through the execution of unauthorized commands via crafted API requests.

Fortinet released updates for affected devices within a week of disclosure to remediate the FortiOS vulnerabilities, advising customers that they may disable SSL VPN as a workaround. However, as of March 2024, about 150,000 public-facing appliances were reported to be at-risk by researchers from the Shadowserver Foundation, with more than 24,000 found in the United States. CISA issued a warning to federal agencies that CSDE-2024-21762 is potentially being exploited in the wild, and that nation-state threat actors and ransomware groups, including Conti and Volt Typhoon, have started targeting Fortinet appliances still impacted by the issue.

As vendors continue to provide updates and report on new vulnerabilities, it is critical to implement best security practices, ensure systems and software are up-to-date, and prioritize continuous management of digital infrastructure as cybercriminals continue to exploit known flaws in systems and software.

The CRITICALSTART® Cyber Research Unit will continue to monitor the situation and work closely with the SOC and Security Engineering team to implement any relevant detections. For future updates the CTI team will post updates via Cyber Operations Risk & Response™ Bulletins and on the CRITICALSTART® Intelligence Hub.

References

1. https://www.theregister.com/2024/03/18/more_than_133000_fortinet_appliances/
2. https://www.cisa.gov/news-events/alerts/2024/02/09/cisa-adds-one-known-exploited-vulnerability-catalog
3. https://arcticwolf.com/resources/blog-uk/cve-2024-21762-and-cve-2024-23113-multiple-critical-vulnerabilities-in-fortinet-one-likely-under-active-exploitation/
4. https://www.bleepingcomputer.com/news/security/critical-fortinet-flaw-may-impact-150-000-exposed-devices/
5. https://www.crn.com/news/security/2024/critical-fortinet-fortios-vulnerability-seeing-exploitation-cisa