Mphasis
The Next Applied

Fortinet - SSL-VPN pre-auth RCE bug is exploited in attacks

Severity: High

Date: 14th Dec 2022

Description

Fortinet urges customers to patch their appliances against an actively exploited FortiOS SSL-VPN vulnerability that could allow unauthenticated remote code execution on devices. Fortinet has patched a zero day buffer overflow in FortiOS that could lead to remote code execution. There has been a report of active exploitation and organizations should patch urgently.

Methodology

The security flaw is tracked as CVE-2022-42475 and is a heap-based buffer overflow bug in FortiOS sslvpnd. When exploited, the flaw could allow unauthenticated users to crash devices remotely and potentially perform code execution.

A heap-based buffer overflow vulnerability [CWE-122] in FortiOS SSL-VPN may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests," warns Fortinet in a security advisory released today.

As reported by LeMagIT, French cybersecurity firm Olympe Cyberdefense first disclosed the Fortinet zero-day vulnerability, warning users to monitor their logs for suspicious activity until a patch was released.

Fortinet quietly fixed the bug on November 28th in FortiOS 7.2.3 (other versions released earlier) without releasing any information about it being exploited as a zero-day.

Today, Fortinet released security advisory FG-IR-22-398, publicly warning that the vulnerability has been actively exploited in attacks and that all users should update to the following versions to fix the bug.

Solution

According to Fortinet's advisory, the following are the affected versions of FortiOS and the relevant fixed versions:

Affected Version	Fixed Version
FortiOS version 7.2.0 through 7.2.2	FortiOS version 7.23 or above
FortiOS version 7.0.0 through 7.0.8	FortiOS version 7.0.9 or above
FortiOS version 6.4.0 through 6.4.10	FortiOS version 6.4.11 or above
FortiOS version 6.2.0 through 6.2.11	FortiOS version 6.2.12 or above
FortiOS version 6.0.0 through 6.0.15	None listed (Added 12/13/2022)
FortiOS version 5.6.0 through 5.6.14	None listed (Added 12/13/2022)
FortiOS version 5.4.0 through 5.4.13	None listed (Added 12/13/2022)
FortiOS version 5.2.0 through 5.2.15	None listed (Added 12/13/2022)
FortiOS version 5.0.0 through 5.0.14	None listed (Added 12/13/2022)
FortiOS-6K7K version 7.0.0 through 7.0.7	FortiOS-6K7K version 7.0.8 or above
FortiOS-6K7K version 6.4.0 through 6.4.9	FortiOS-6K7K version 6.4.10 or above
FortiOS-6K7K version 6.2.0 through 6.2.11	FortiOS-6K7K version 6.2.12 or above
FortiOS-6K7K version 6.0.0 through 6.0.14	FortiOS-6K7K version 6.0.15 or above

IOC's

Fortinet also shared a list of IP addresses seen exploiting the vulnerability, listed below

- 188.34.130.40:444
- 103.131.189.143:30080,30081,30443,20443
- 192.36.119.61:8443,444
- 172.247.168.153:8033

Reference Links

- https://www.bleepingcomputer.com/news/security/fortinet-says-ssl-vpn-pre-auth-rce-bug-is-exploited-in- attacks/
- https://www.tenable.com/blog/cve-2022-42475-fortinet-patches-zero-day-in-fortios-ssl-vpns?utm_source=cyber_exposure_alerts_community&utm_medium=community&utm_campaign=tenable_community