February 9, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a FortiOS SSL VPN vulnerability. The vulnerability affects versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17, FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7.

Technical Details

Fortinet is warning that a new critical remote code execution vulnerability in FortiOS SSL VPN is potentially being exploited in attacks.

An out-of-bounds write vulnerability in FortiOS may allow an attacker to execute unauthorized code or commands via specifically crafted requests. For those unable to apply patches, you can mitigate the flaw by disabling SSL VPN on your FortiOS devices.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-21762
- FortiOS - Out-of-bound Write in sslvpnd
- New Fortinet RCE flaw in SSL VPN likely exploited in attacks
- VRM Vulnerability Reports