deepwatch

12.13.22

Customer Advisory: FortiOS SSL-VPN Vulnerability (CVE-2022-42475) Exploited in the Wild

By  Eric Ford, Sr. Threat Intelligence Analyst

Estimated Reading Time: 4 minutes

Executive Summary

On 12 December, Fortinet published an **advisory** warning organizations of a vulnerability in FortiOS SSL-VPN products. In the advisory, Fortinet states that they know the vulnerability has been actively exploited in the wild in at least one instance.

The vulnerability affects several versions of FortiOS and FortiOS-6K7K. It is due to a heap-based buffer overflow that allows a **remote unauthenticated** threat actor the ability to **execute arbitrary code or commands**. The vulnerability is tracked as CVE-2022-42475 and has a **CVSSv3 score of 9.3**.

FortiOS SSL-VPNs are typically internet-facing, offering threat actors easy access to organizational networks. Organizations using one of the affected versions of FortiOS are at risk of threat actors exploiting this vulnerability. Threat actors have exploited FortiOS vulnerabilities in the past, deploying ransomware and selling the access on criminal marketplaces.

Key Findings

- FortiOS SSL-VPN products are vulnerable to a heap-based buffer overflow. The vulnerability has been assigned CVE-2022-42475 with a CVSSv3 score of 9.3.
- Fortinet knows at least one instance where threat actors exploited this vulnerability in the wild.
- FortiOS SSL-VPNs are typically internet-facing, offering threat actors easy access to organizational networks.
- Fortinet has provided indicators of compromise observed in the exploitation of the vulnerability.

via specifically crafted requests.

Affected Versions:

- FortiOS version 7.2.0 through 7.2.2
- FortiOS version 7.0.0 through 7.0.8
- FortiOS version 6.4.0 through 6.4.10
- FortiOS version 6.2.0 through 6.2.11
- FortiOS version 6.0.0 through 6.0.15
- FortiOS version 5.6.0 through 5.6.14
- FortiOS version 5.4.0 through 5.4.13
- FortiOS version 5.2.0 through 5.2.15
- FortiOS version 5.0.0 through 5.0.14
- FortiOS-6K7K version 7.0.0 through 7.0.7
- FortiOS-6K7K version 6.4.0 through 6.4.9
- FortiOS-6K7K version 6.2.0 through 6.2.11
- FortiOS-6K7K version 6.0.0 through 6.0.14

Why You Should Act?

FortiOS SSL-VPNs are typically internet-facing, offering threat actors easy access to organizational networks. Organizations using one of the affected versions of FortiOS found in the "**Affected Products**" section of the advisory are at risk of threat actors exploiting this vulnerability. It is essential to take action immediately to protect your systems and data from attack.

Threat Actors Exploited FortiOS in the Past

In late November, **Cyble** published a report detailing a threat actor was selling access to multiple organizations they obtained by exploiting another vulnerability in FortiOS devices. In another case, **Symantec** detailed in a report published in late April how ransomware threat actors exploited another vulnerability in FortiOS to gain initial access.

What Will Adversaries Do Next?

Threat actors will likely continue to exploit this vulnerability in the wild until it is patched. They could develop new methods of exploiting the vulnerability. However, we can not rule out the possibility that they could combine it with other vulnerabilities to create even more destructive attacks.

As seen in previous cases, threat actors could sell the access gained from exploiting the vulnerability on

- Deepwatch Vulnerability Management (VM) service customers received additional details from your VM engineer.
- Deepwatch conducts further detection assessments and threat hunting from data reported in our intelligence reports. However, not all activity can be hunted, detected, or monitored due to limitations in log sources received by Deepwatch. If you have questions about which log sources you should be ingesting to hunt, detect, and monitor the relevant intelligence from this report, please direct your inquiry to your respective squad manager.

Be On the Lookout (BOLO)

According to Fortinet, organizations should audit and monitor their devices for the following indicators and artifacts:

- Multiple log entries with:
- Logdesc="Application crashed" and msg="[…] application:sslvpnd,[…], Signal 11 received, Backtrace: […]"
- Presence of the following artifacts in the filesystem:
  - /data/lib/libips.bak
  - /data/lib/libgif.so
  - /data/lib/libiptcp.so
  - /data/lib/libipudp.so
  - /data/lib/libjepg.so
  - /var/.sslvpnconfigbk
  - /data/etc/wxd.conf
  - /flash
- Connections to the following IP addresses or suspicious IP addresses from the FortiGate:
  - 188.34.130.40:444 [Germany; Hetzner Online AG]
  - 103.131.189.143:30080,30081, 30443, and 20443 [Taiwan; Soon Keat Neo]
  - 192.36.119.61:8443 and 444 [Sweden; Resilans AB]
  - 172.247.168.153:8033 [USA; CloudRadium L.L.C]

Subscribe to the Deepwatch Insights Blog

deepwatch

Deepwatch® is the leading managed security platform for the cyber resilient enterprise. Our platform combines comprehensive threat management capabilities, Deepwatch security experts, and precise automated actions to enable cyber resiliency and reduce risk.

Corporate Headquarters

4030 W Boy Scout Blvd.
Suite 550
Tampa, FL 33607 USA
855.303.3033
info@deepwatch.com

Company

Our Customers

Security Center

Platform

Solution Providers

Strategic Alliance Partners

About

Leadership

Careers

Trust

Contact Us

Resources

Threat Intelligence

Resource Library

Blog

Press

Events

Customer Login

Sitemap | Privacy Policy