Fortinet FortiOS 7.2.2 SSL-VPN Heap-Based Buffer Overflow Vulnerability

Vulnerability (VU)

December 12, 2022 09:18:16 PM, 22-00027349, Version: 1 Risk Rating: HIGH | Exploitation State: Confirmed

Executive Summary

A heap-based buffer overflow vulnerability exists within the SSL-VPN component Fortinet FortiOS 7.2.2 and earlier that, when exploited, allows a remote attacker to execute arbitrary code. Exploit code is not publicly available, but exploitation of the vulnerability in the wild has been reported. Mitigation options include a vendor fix.

Description

Fortinet has provided the following description:
A heap-based buffer overflow vulnerability in FortiOS SSL-VPN may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests.

Date of Disclosure

December 12, 2022 07:00:00 AM

Threat Detail

An attacker could exploit this vulnerability to execute arbitrary code. An attacker would need to send a specially crafted request. A failed attempt at exploitation could potentially cause a crash of the application, resulting in a denial-of-service condition.

Fortinet has reported that they are aware of this vulnerability being leveraged in the wild.

Mandiant Intelligence considers this a High-risk vulnerability due to the potential for arbitrary code execution with little to no user interaction or privileges required.

Please rate this product by taking a short four question survey

Vulnerable Products

The following vendors/products have been reported as vulnerable:

- Fortinet, Inc.: FortiOS 6.2.0, 6.2.1, 6.2.2, 6.2.3, 6.2.4, 6.2.5, 6.2.6, 6.2.7, 6.2.8, 6.2.9, 6.2.10, 6.2.11, 6.4.0, 6.4.1, 6.4.2, 6.4.3, 6.4.4, 6.4.5, 6.4.6, 6.4.7, 6.4.8, 6.4.9, 6.4.10, 7.0.0, 7.0.1, 7.0.2, 7.0.3, 7.0.4, 7.0.5, 7.0.6, 7.0.7, 7.0.8, 7.2.0, 7.2.1, and 7.2.2

First Version Publish Date

December 12, 2022 09:18:16 PM

Exploitation

In the wild	true
Zero Day	true

Technical Tags

Attacking Ease	Easy
Exploitation Vectors	• General Network Connectivity
Exploitation Consequence	Code Execution
Exploitation State	Confirmed
Mitigation	• Patch
Vulnerability Type	Heap-based Buffer Overflow

Common Vulnerabilities (CVSS V2)

CVSSBaseScore:	10
CVSSTemporalScore:	8.3
Access Vector	AV:N
Access Complexity	AC:L
Authentication	Au:N
Confidentiality Impact	C:C
Integrity Impact	I:C
Availability Impact	A:C
Exploitability	E:F
Remediation	RL:OF
Report Confidence	RC:C

Sources

Title:	Fortinet, Inc.
Source URL:	hxxps://fortiguard[.]fortinet[.]com/psirt/FG-IR-22-398
Date:	December 12, 2022 11:00:00 PM
Description:	FortiOS - heap-based buffer overflow in sslvpnd

Version Information

Version:1, December 12, 2022 09:18:16 PM

Technology

Vendor - Technology	CPE
fortinet - fortios 6.2.0	cpe:2.3:o:fortinet:fortios:6.2.0:*:*:*:*:*:*:*
fortinet - fortios 6.2.10	cpe:2.3:o:fortinet:fortios:6.2.10:*:*:*:*:*:*:*
fortinet - fortios 6.2.11	cpe:2.3:o:fortinet:fortios:6.2.11:*:*:*:*:*:*:*
fortinet - fortios 6.2.1	cpe:2.3:o:fortinet:fortios:6.2.1:*:*:*:*:*:*:*
fortinet - fortios 6.2.2	cpe:2.3:o:fortinet:fortios:6.2.2:*:*:*:*:*:*:*
fortinet - fortios 6.2.3	cpe:2.3:o:fortinet:fortios:6.2.3:*:*:*:*:*:*:*
fortinet - fortios 6.2.4	cpe:2.3:o:fortinet:fortios:6.2.4:*:*:*:*:*:*:*
fortinet - fortios 6.2.5	cpe:2.3:o:fortinet:fortios:6.2.5:*:*:*:*:*:*:*

fortinet - fortios 6.2.6	cpe:2.3:o:fortinet:fortios:6.2.6:*:*:*:*:*:*:*
fortinet - fortios 6.2.7	cpe:2.3:o:fortinet:fortios:6.2.7:*:*:*:*:*:*:*
fortinet - fortios 6.2.8	cpe:2.3:o:fortinet:fortios:6.2.8:*:*:*:*:*:*:*
fortinet - fortios 6.2.9	cpe:2.3:o:fortinet:fortios:6.2.9:*:*:*:*:*:*:*
fortinet - fortios 6.4.0	cpe:2.3:o:fortinet:fortios:6.4.0:*:*:*:*:*:*:*
fortinet - fortios 6.4.1	cpe:2.3:o:fortinet:fortios:6.4.1:*:*:*:*:*:*:*
fortinet - fortios 6.4.2	cpe:2.3:o:fortinet:fortios:6.4.2:*:*:*:*:*:*:*
fortinet - fortios 6.4.3	cpe:2.3:o:fortinet:fortios:6.4.3:*:*:*:*:*:*:*
fortinet - fortios 6.4.4	cpe:2.3:o:fortinet:fortios:6.4.4:*:*:*:*:*:*:*
fortinet - fortios 6.4.5	cpe:2.3:o:fortinet:fortios:6.4.5:*:*:*:*:*:*:*
fortinet - fortios 6.4.6	cpe:2.3:o:fortinet:fortios:6.4.6:*:*:*:*:*:*:*
fortinet - fortios 6.4.7	cpe:2.3:o:fortinet:fortios:6.4.7:*:*:*:*:*:*:*
fortinet - fortios 6.4.8	cpe:2.3:o:fortinet:fortios:6.4.8:*:*:*:*:*:*:*
fortinet - fortios 6.4.9	cpe:2.3:o:fortinet:fortios:6.4.9:*:*:*:*:*:*:*
fortinet - fortios 7.0.0	cpe:2.3:o:fortinet:fortios:7.0.0:*:*:*:*:*:*:*
fortinet - fortios 7.0.1	cpe:2.3:o:fortinet:fortios:7.0.1:*:*:*:*:*:*:*
fortinet - fortios 7.0.2	cpe:2.3:o:fortinet:fortios:7.0.2:*:*:*:*:*:*:*
fortinet - fortios 7.0.3	cpe:2.3:o:fortinet:fortios:7.0.3:*:*:*:*:*:*:*
fortinet - fortios 7.0.4	cpe:2.3:o:fortinet:fortios:7.0.4:*:*:*:*:*:*:*
fortinet - fortios 7.0.5	cpe:2.3:o:fortinet:fortios:7.0.5:*:*:*:*:*:*:*
fortinet - fortios 7.0.6	cpe:2.3:o:fortinet:fortios:7.0.6:*:*:*:*:*:*:*
fortinet - fortios 7.0.7	cpe:2.3:o:fortinet:fortios:7.0.7:*:*:*:*:*:*:*
fortinet - fortios 7.0.8	cpe:2.3:o:fortinet:fortios:7.0.8:*:*:*:*:*:*:*
fortinet - fortios 7.2.0	cpe:2.3:o:fortinet:fortios:7.2.0:*:*:*:*:*:*:*
fortinet - fortios 7.2.1	cpe:2.3:o:fortinet:fortios:7.2.1:*:*:*:*:*:*:*
fortinet - fortios 7.2.2	cpe:2.3:o:fortinet:fortios:7.2.2:*:*:*:*:*:*:*

Common Vulnerabilities and Exposures

CVE ID:	CVE-2022-42475(CVE Description)Mandiant Vulnerability Analysis