



CVE-2023-22640

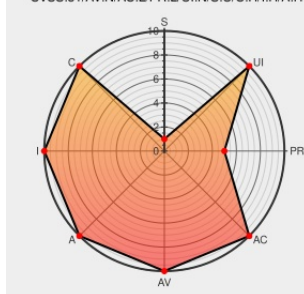
Published on: Not Yet Published

Last Modified on: 05/10/2023 09:10:00 PM UTC

CVE-2023-22640

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Fortios](#) from [Fortinet](#) contain the following vulnerability:

A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy

all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted requests.

CVE-2023-22640 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
PSIRT Advisories FortiGuard	fortiguard.com text/html	MISC fortiguard.com/psirt/FG-IR-22-475

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](#).

Related QID Numbers

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fortinet	Fortios	All	All	All	All
Operating System	Fortinet	Fortios	All	All	All	All
Application	Fortinet	Fortiproxy	1.0.0	All	All	All
Application	Fortinet	Fortiproxy	1.1.0	All	All	All
Application	Fortinet	Fortiproxy	1.2.0	All	All	All
Application	Fortinet	Fortiproxy	2.0.0	All	All	All

cpe:2.3:o:fortinet:fortios:*****:

cpe:2.3:o:fortinet:fortios:*****:

cpe:2.3:a:fortinet:fortiproxy:1.0.0:*****:

cpe:2.3:a:fortinet:fortiproxy:1.1.0:*****:

cpe:2.3:a:fortinet:fortiproxy:1.2.0:*****:

cpe:2.3:a:fortinet:fortiproxy:2.0.0:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-22640 : A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 throu... twitter.com/i/web/status/1...	2023-05-03 22:06:20
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2023-22640 A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7... twitter.com/i/web/status/1...	2023-05-03 23:11:02
 @RedPacketSec	Fortinet FortiOS and FortiProxy code execution CVE-2023-22640 - redpacketsecurity.com/fortinet-forti... #CVE #Vulnerability #OSINT #ThreatIntel #Cyber	2023-05-05 09:03:52
 @ohhara_shiojiri	CVE - CVE-2023-22640	2023-05-05 10:15:29
 @ohhara_shiojiri	"The second high-severity flaw, CVE-2023-22640, is described as an out-of-bounds write in the sslvpng component of FortiOS and FortiProxy."	2023-05-05 13:24:22
 @ka0com	>CVE-2023-27999 の欠陥 (CVSS スコア 7.6) は、外部リソース モジュールでのコマンド インジェクションの問題です。 >CVE-2023-22640 の欠陥 (CVSS スコア 7.1) は、FortiOS... twitter.com/i/web/status/1...	2023-05-05 23:50:33

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)