



CVE-2022-38725

Published on: Not Yet Published

Last Modified on: 02/03/2023 04:52:00 PM UTC

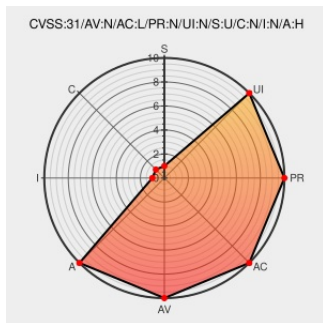
CVE-2022-38725

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Syslog-ng](#) from [Oneidentity](#) contain the following vulnerability:

An integer overflow in the RFC3164 parser in One Identity syslog-ng 3.0 through 3.37 allows remote attackers to cause a Denial of Service via crafted syslog input that is mishandled by the tcp or network function. syslog-ng Premium Edition 7.0.30 and syslog-ng Store Box 6.10.0 are also affected.

CVE-2022-38725 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
An integer overflow in the RFC3164 parser allows remote attackers Denial of Service · Advisory · syslog-ng/syslog-ng · GitHub	github.com text/html	MISC github.com/syslog-ng/syslog-ng/security/advisories/GHSA-7932-4fc6-pvmc
The syslog-ng Archives	lists.balabit.hu text/html	MISC lists.balabit.hu/pipermail/syslog-ng/

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

905376 Common Base Linux Mariner (CBL-Mariner) Security Update for syslog-ng (13198)

905379 Common Base Linux Mariner (CBL-Mariner) Security Update for syslog-ng (13205)

Exploit/POC from Github

An integer overflow in the RFC3164 parser in One Identity syslog-ng 3.0 through 3.37 allows remote attackers to cause...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oneidentity	Syslog-ng	All	All	All	All
Application	Oneidentity	Syslog-ng	All	All	All	All
Application	Oneidentity	Syslog-ng Store Box	All	All	All	All
Application	Oneidentity	Syslog-ng Store Box	All	All	All	All

[cpe:2.3:a:oneidentity:syslog-ng.*.*.*.*.*.*.*.*](#)

[cpe:2.3:a:oneidentity:syslog-ng.*.*.*.*.premium.*.*.*](#)

[cpe:2.3:a:oneidentity:syslog-ng_store_box.*.*.*.*.*.*.*.*](#)

[cpe:2.3:a:oneidentity:syslog-ng_store_box.*.*.*.*.lts.*.*.*](#)

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVereport	CVE-2022-38725 : An integer overflow in the RFC3164 parser in One Identity syslog-ng 3.0 through 3.37 allows remote... twitter.com/i/web/status/1...	2023-01-23 16:05:07
/r/netcve	CVE-2022-38725	2023-01-23 16:40:19

[← 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](#)