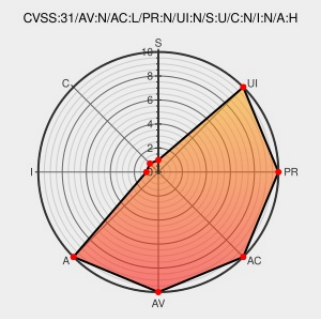
CVE-2022-38725

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 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/

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→