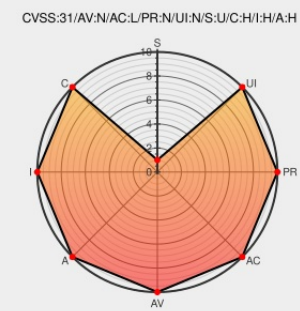
CVE-2022-4779

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:21:00 PM UTC

CVE-2022-4779

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Streamx from Elvexys contain the following vulnerability:

StreamX applications from versions 6.02.01 to 6.04.34 are affected by a logic bug that allows to bypass the implemented authentication scheme. StreamX applications using StreamView HTML component with the public web server feature activated are affected.

CVE-2022-4779 has been assigned by vulnerability@ncsc.ch to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **elvexys** - **StreamX** version **= 6.02.01**

CVSS3 Score: 9.8 - CRITICAL

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

CVE References

Description	Tags	Link
StreamX release notes - Elvexys SA	elvexys.com text/html	MISC elvexys.com/products/xpg-gateway-rtu-protocol-converter/streamx-release-notes/

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Exploit/POC from Github

StreamX applications from versions 6.02.01 to 6.04.34 are affected by a logic bug that allows to bypass the implement…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Elvexys	Streamx	All	All	All	All

cpe:2.3:a:elvexys:streamx:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-4779 : StreamX applications from versions 6.02.01 to 6.04.34 are affected by a logic bug that allows to by… twitter.com/i/web/status/1…	2022-12-29 00:04:07
/r/netcve	CVE-2022-4779	2022-12-29 00:38:31

← Previous ID

Next ID→