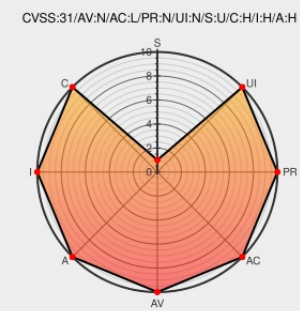
CVE-2023-25076

Published on: Not Yet Published

Last Modified on: 05/27/2023 04:15:00 AM UTC

CVE-2023-25076

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



Certain versions of Sniproxy from Sniproxy Project contain the following vulnerability:

A buffer overflow vulnerability exists in the handling of wildcard backend hosts of SNIProxy 0.6.0-2 and the master branch (commit: 822bb80df9b7b345cc9eba55df74a07b498819ba). A specially crafted HTTP or TLS packet can lead to arbitrary code execution. An attacker could send a malicious packet to trigger this vulnerability.

CVE-2023-25076 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **SNIProxy** - **SNIProxy** version **= 0.6.0-2**

Affected Vendor/Software: **SNIProxy** - **SNIProxy** version **= Master 822bb80df9b7b345cc9eba55df74a07b498819ba**

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
TALOS-2023-1731 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2023-1731
Debian -- Security Information -- DSA-5413-1 sniproxy	www.debian.org Depreciated Link text/html	MISC www.debian.org/security/2023/dsa-5413
[SECURITY] [DLA 3406-1]	lists.debian.org	MISC lists.debian.org/debian-lts-announce/2023/04/msg00030.html

sniproxy security update	text/html	
address: fix buffer overflow · dlundquist/sniproxy@f8d9a43 · GitHub	github.com text/html	MISC github.com/dlundquist/sniproxy/commit/f8d9a433fe22ab2fa15c00179048ab02ae23d58

Related QID Numbers

181755 Debian Security Update for sniproxy (DLA 3406-1)

181804 Debian Security Update for sniproxy (DSA 5413-1)

184235 Debian Security Update for sniproxy (CVE-2023-25076)

199410 Ubuntu Security Notification for SNI Proxy Vulnerability (USN-6148-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sniproxy Project	Sniproxy	0.6.0-2	All	All	All
Application	Sniproxy Project	Sniproxy	0.6.1	All	All	All

cpe:2.3:a:sniproxy_project:sniproxy:0.6.0-2:*:*:*:*:*:*:*:

cpe:2.3:a:sniproxy_project:sniproxy:0.6.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-25076 : A buffer overflow vulnerability exists in the handling of wildcard backend hosts of SNIProxy 0.6.0… twitter.com/i/web/status/1…	2023-03-30 15:06:05
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2023-25076 A buffer overflow vulnerability exists in the handling of wildcar… twitter.com/i/web/status/1…	2023-03-30 16:11:00
/r/netcve	CVE-2023-25076	2023-03-30 16:38:38

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report