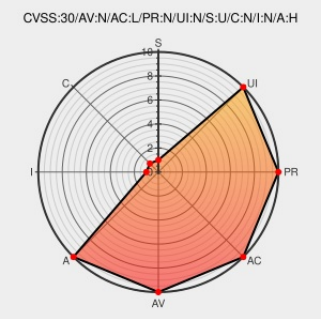
CVE-2020-6060

Published on: 02/04/2020 12:00:00 AM UTC

Last Modified on: 06/07/2022 04:51:00 PM UTC

CVE-2020-6060

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



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

A stack buffer overflow vulnerability exists in the way MiniSNMPD version 1.4 handles multiple connections. A specially timed sequence of SNMP connections can trigger a stack overflow, resulting in a denial of service. To trigger this vulnerability, an attacker needs to simply initiate multiple connections to the server.

CVE-2020-6060 has been assigned by talos-cna@cisco.com 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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
TALOS-2020-0977 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	www.talosintelligence.com text/html	MISC www.talosintelligence.com/vulnerability_reports/TALOS-2020-0977

TALOS-2019-0977 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Third Party Advisory talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2019-0977

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Minisnmpd Project	Minisnmpd	1.4	All	All	All
Application	Minisnmpd Project	Minisnmpd	1.4	All	All	All

cpe:2.3:a:minisnmpd_project:minisnmpd:1.4:*:*:*:*:*:*:*:

cpe:2.3:a:minisnmpd_project:minisnmpd:1.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→