NET-SNMP- VULNERABILITIES

PUBLISHED: NOVEMBER 08, 2022 | LAST UPDATE: NOVEMBER 08, 2022

Summary

A number of Net-SNMP vulnerabilities can impact management plane services on ACOS devices that can cause crashes SNMP services in ACOS devices resulting in potential, transient Denial-of Service (DoS) or other security impacts by malicious SNMP actors. These vulnerabilities are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2019-20892	CVSSv3	6.5 Med	net-snmp: double free in usm_free_usmStateReference function in snmplib/snmpusm.c via an SNMPv3 GetBulk request
2	CVE-2018-18065	CVSSv3	6.5 Med	net-snmp: NULL pointer exception in _set_key in agent/helpers/table_container.c resulting in a denial of service
3	CVE-2018-18066	CVSSv3	7.5 High	net-snmp: NULL pointer exception in snmp_oid_compare in snmplib/snmp_api.c resulting in a denial of service
4	CVE-2012-6151	CVSSv2	4.3 Med	net-snmp: snmpd crashes/hangs when AgentX subagent times-out
5	CVE-2012-2141	CVSSv2	3.5 Low	net-snmp: Array index error, leading to out-of heap-based buffer read (snmpd crash)

Affected Releases

The table below indicates releases of ACOS exposed to this vulnerability and ACOS releases that address them. ACOS release families not indicated below are unaffected by these vulnerabilities.

Customers using affected ACOS releases can overcome vulnerability exposures by updating to the indicated resolved release. If the table does not list a corresponding resolved or unaffected release, then no ACOS release update is currently available.

Releases Affected			Releases Resolved or Unaffected
5.0.0	–	5.2.1-P6	5.2.1-P7
5.0.1 TPS	–	5.0.2-P2 TPS	5.0.2-P3-TPS
4.1.4-GR1	–	4.1.4-GR1-P11	4.1.4-GR1-P12
3.2.3-P1	–	3.2.5-P6	5.0.2-P3 TPS

Workarounds and Mitigations

None

Software Updates

Software updates that address these vulnerabilities are or will be published at the following URL:

https://support.a10networks.com/

Vulnerability Details

The following table shares brief descriptions for the vulnerabilities addressed in this document.

Vulnerability ID	Description
CVE-2019-20892	net-snmp before 5.8.1.pre1 has a double free in usm_free_usmStateReference in snmplib/snmpusm.c via an SNMPv3 GetBulk request. NOTE: this affects net-snmp packages shipped to end users by multiple Linux distributions, but might not affect an upstream release.
CVE-2018-18065	_set_key in agent/helpers/table_container.c in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an authenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.
CVE-2018-18066	snmp_oid_compare in snmplib/snmp_api.c in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an unauthenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.
CVE-2012-6151	Net-SNMP 5.7.1 and earlier, when AgentX is registering to handle a MIB and processing GETNEXT requests, allows remote attackers to cause a denial of service (crash or infinite loop, CPU consumption, and hang) by causing the AgentX subagent to timeout.
CVE-2012-2141	Array index error in the handle_nsExtendOutput2Table function in agent/mibgroup/agent/extend.c in Net-SNMP 5.7.1 allows remote authenticated users to cause a denial of service (out-of-bounds read and snmpd crash) via an SNMP GET request for an entry not in the extension table.

Related Links

Ref #	General Link
[1]	NIST NVD, CVE-2019-20892
[2]	NIST NVD, CVE-2018-18065
[3]	NIST NVD, CVE-2018-18066
[4]	NIST NVD, CVE-2012-6151
[5]	NIST NVD, CVE-2012-2141

Acknowledgements

None

Modification History

Revision	Date	Description
1.0	2022-11-08	Initial Publication

This document is provided on an "AS IS" basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability, non-infringement or fitness for a particular use. Your use of the information in this document or materials linked from this document is at your own risk. A10 Networks, Inc. reserves the right to change or update the information in this document at any time.