SECURITY BULLETIN 2024-2

SNMP Manager vulnerabilities

SUMMARY :

This document contains information about a vulnerability affecting the SNMP Manager component

Reference	SB2024-2
Publication date	2024.11.21
Last update	2024.11.21
Confidentiality	**TLP:CLEAR**

Date	Revision	Action
2024.11.21	1.0	Initial version

1. Overview

ARC Informatique is aware of security vulnerabilities affecting PcVue.

The affected component is the Net-SNMP library used in PcVue for the SNMP Manager component.

Multiple vulnerabilities, listed below, have been reported on this library. Those that might affect the product are highlighted.

CVE Id	Title
CVE-2022-44793	handle_ipv6IpForwarding in agent/mibgroup/ip-mib/ip_scalars.c in Net-SNMP 5.4.3 through 5.9.3 has a NULL Pointer Exception bug that can be used by a remote attacker to cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.
CVE-2022-44792	handle_ipDefaultTTL in agent/mibgroup/ip-mib/ip_scalars.c in Net-SNMP 5.8 through 5.9.3 has a NULL Pointer Exception bug that can be used by a remote attacker (who has write access) to cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.
CVE-2022-24810	net-snmp provides various tools relating to the Simple Network Management Protocol. Prior to version 5.9.2, a user with read-write credentials can use a malformed OID in a SET to the nsVacmAccessTable to cause a NULL pointer dereference. Version 5.9.2 contains a patch. Users should use strong SNMPv3 credentials and avoid sharing the credentials. Those who must use SNMPv1 or SNMPv2c should use a complex community string and enhance the protection by restricting access to a given IP address range.
CVE-2022-24809	net-snmp provides various tools relating to the Simple Network Management Protocol. Prior to version 5.9.2, a user with read-only credentials can use a malformed OID in a `GET-NEXT` to the `nsVacmAccessTable` to cause a NULL pointer dereference. Version 5.9.2 contains a patch. Users should use strong SNMPv3 credentials and avoid sharing the credentials. Those who must use SNMPv1 or SNMPv2c should use a complex community string and enhance the protection by restricting access to a given IP address range.
CVE-2022-24808	net-snmp provides various tools relating to the Simple Network Management Protocol. Prior to version 5.9.2, a user with read-write credentials can use a malformed OID in a `SET` request to `NET-SNMP-AGENT-MIB::nsLogTable` to cause a NULL pointer dereference. Version 5.9.2 contains a patch. Users should use strong SNMPv3 credentials and avoid sharing the credentials. Those who must use SNMPv1 or SNMPv2c should use a complex community string and enhance the protection by restricting access to a given IP address range.
CVE-2022-24807	net-snmp provides various tools relating to the Simple Network Management Protocol. Prior to version 5.9.2, a malformed OID in a SET request to `SNMP-VIEW-BASED-ACM-MIB::vacmAccessTable` can cause an out-of-bounds memory access. A user with read-write credentials can exploit the issue. Version 5.9.2 contains a patch. Users should use strong SNMPv3 credentials and avoid sharing the credentials. Those who must use SNMPv1 or SNMPv2c should use a complex community string and enhance the protection by restricting access to a given IP address range.
CVE-2022-24806	net-snmp provides various tools relating to the Simple Network Management Protocol. Prior to version 5.9.2, a user with read-write credentials can exploit an Improper Input Validation vulnerability when SETing malformed OIDs in master agent and subagent simultaneously. Version 5.9.2 contains a patch. Users should use strong SNMPv3 credentials and avoid sharing the credentials. Those who must use SNMPv1 or SNMPv2c should use a complex community string and enhance the protection by restricting access to a given IP address range.

CVE Id	Title
CVE-2022-24805	net-snmp provides various tools relating to the Simple Network Management Protocol. Prior to version 5.9.2, a buffer overflow in the handling of the `INDEX` of `NET-SNMP-VACM-MIB` can cause an out-of-bounds memory access. A user with read-only credentials can exploit the issue. Version 5.9.2 contains a patch. Users should use strong SNMPv3 credentials and avoid sharing the credentials. Those who must use SNMPv1 or SNMPv2c should use a complex community string and enhance the protection by restricting access to a given IP address range.
CVE-2020-15862	Net-SNMP through 5.8 has Improper Privilege Management because SNMP WRITE access to the EXTEND MIB provides the ability to run arbitrary commands as root.
CVE-2020-15861	Net-SNMP through 5.7.3 allows Escalation of Privileges because of UNIX symbolic link (symlink) following.
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-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-2018-1000116	NET-SNMP version 5.7.2 contains a heap corruption vulnerability in the UDP protocol handler that can result in command execution.
CVE-2015-5621	The snmp_pdu_parse function in snmp_api.c in net-snmp 5.7.2 and earlier does not remove the varBind variable in a netsnmp_variable_list item when parsing of the SNMP PDU fails, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted packet.

This bulletin describes the immediate security measures to prevent the malicious exploitation of this vulnerability. We strongly recommend that users of the affected products apply these measures.

2. Affected products and components

Component	Product & Versions	Description
SNMP Manager	PcVue 12 PcVue 15 PcVue 16	Use of a vulnerable version of the Net-SNMP library

3. Impact

Successful exploitation of these vulnerabilities could lead to a disclosure of sensitive information, or addition or modification of data.

The exact impact on a particular system depends on many factors. According to the vulnerabilities described hereafter, we recommend that each user of the affected products evaluates the risk for their system.

4. Vulnerability details

4.1 Improper Privilege Management

CVE Id	CVE-2020-15862			
Publication date	2020-08-19			
Description	Net-SNMP through 5.8 has Improper Privilege Management because SNMP WRITE access to the EXTEND MIB provides the ability to run arbitrary commands as root.			
CVSS v3.1 Base Score	7.8			
CVSS v3.1 Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H			
Attack Vector	Network	Adjacent	Local	Physical
Attack Complexity	Low		High	
Privileges Required	None	Low	High	
User interaction	None		Required	
Scope	Changed		Unchanged	
Confidentiality	High	Low	None	
Integrity	High	Low	None	
Availability	High	Low	None	
CWE Ids	CWE-269 – Improper Privilege Management			

4.2 Improper Link Resolution

CVE Id	CVE-2020-15861			
Publication date	2020-08-19			
Description	Net-SNMP through 5.7.3 allows Escalation of Privileges because of UNIX symbolic link (symlink) following.			
CVSS v3.1 Base Score	7.8			
CVSS v3.1 Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H			
Attack Vector	Network	Adjacent	Local	Physical
Attack Complexity	Low		High	
Privileges Required	None	Low	High	
User interaction	None		Required	
Scope	Changed		Unchanged	
Confidentiality	High	Low	None	
Integrity	High	Low	None	
Availability	High	Low	None	
CWE Ids	CWE-59 – Improper Link Resolution Before File Access (‘Link Following’)			

5. Immediate risk mitigation

5.1 Harden the configuration

Who should apply this recommendation: All users
The system operators are highly recommended to take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the Internet unless required.
- Locate control system networks and remote devices behind firewalls and isolate them from business networks.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its connected devices.
- Operate PcVue with a standard user. Administrative rights are only required at installation or for deployment purposes.

5.2 Update PcVue

Who should apply this recommendation: All users using the affected component
Apply the patch by installing a fixed PcVue version.

6. Available patches

Component	Product
SNMP Manager	Fixed in: • PcVue 16.2.1 – with Net-SNMP 5.9.4

7. Credits

N/A

8. References

The public ARC Informatique security alert page: www.pcvue.com/security

CVE:
- CVE-2020-15862
- CVE-2020-15861

Want to report a vulnerability or provide feedback – Please email us at secure@arcinfo.com

SECURITY BULLETIN

2024-2

ARC Informatique
Private limited company
capitalized at 1 250 000 €
RCS Nanterre B 320 695 356
APE 5829C / SIREN 320 695 356
VAT N°FR 19320695 356

Headquarters
2 avenue de la Cristallerie,
92310 Sèvres, France
Tél: +33 1 41 14 36 00
Hotline: +33 1 41 14 36 25
Email: arcnews@arcinfo.com
www.pcvue.com

ARC Informatique is
ISO 9001, ISO 14001 and
ISO 27001 certified

We would love to hear your thoughts and suggestions
so we can improve this document
Contact us at secure@arcinfo.com