SICK PSIRT
Security Advisory

Package Analytics affected by Windows TCP/IP vulnerability

Document ID:	SCA-2020-0005
Publication Date:	2020-10-29
CVE Identifier:	CVE-2020-16898
CVSSv3 Base Score:	8.8
CVSSv3 Vector String:	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
Version:	2

Summary

Microsoft disclosed a critical vulnerability in the way ICMPv6 Router Advertisement packets are handled on Windows 10 and Windows Server 2019. An attacker who successfully exploited this vulnerability could gain the ability to execute code on the target server or client. To exploit this vulnerability, an attacker would have to send specially crafted ICMPv6 Router Advertisement packets to a remote Windows computer.

All Package Analytics versions 4.0 to 4.1.2, which run on PCs containing the affected Windows OS, will be affected. However there are instances of PA running on older versions of Windows such as Windows 7, Windows Server 2012 R2, Windows Server 2016 R2 which do not appear in the list of affected OS for this issue.

List of Products

Product	**Affected by**
SICK Package Analytics 4.0 up to 4.1.2	CVE-2020-16898 Status: Known Affected Remediation: Vendor fix, Mitigation

Vulnerability Overview

CVE-2020-16898

CVE description: A remote code execution vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets, aka 'Windows TCP/IP Remote Code Execution Vulnerability'.

CVE-2020-16898 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.8
CVSSv3.1 vector string: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

References:
Microsoft Security Advisory:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898

Remediations

Vendor Fix for CVE-2020-16898

Details: This issue is addressed in the Microsoft update for CVE-2020-16898.

URL: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898

Valid for:

- SICK Package Analytics 4.0 up to 4.1.2

Mitigation for CVE-2020-16898

Details: If you find yourself in a situation where an update is not doable. Microsoft advises the following workarounds:
Disable ICMPv6 RDNSS:
The following workaround may be helpful in your situation. In all cases, Microsoft strongly recommends that you install the updates for this vulnerability as soon as they become available even if you plan to leave this workaround in place:
You can check your *INTERFACENUMBER* by running this command in a cmd:

```
route print
```

You can disable ICMPv6 RDNSS, to prevent attackers from exploiting the vulnerability, with the PowerShell command below. This workaround is only available for Windows 1709 and above. See What's new in Windows Server 1709 for more information.

```
netsh int ipv6 set int *INTERFACENUMBER* rabaseddnsconfig=disable
```

Note: No reboot is needed after making the change.
You can disable the workaround with the PowerShell command below.

```
netsh int ipv6 set int *INTERFACENUMBER* rabaseddnsconfig=enable
```

Note: No reboot is needed after disabling the workaround.
Package Analytics has been verified to function without any issue and is compatible with the prescribed Microsoft update. No additional PA patches are necessary.

Valid for:

- SICK Package Analytics 4.0 up to 4.1.2

General Security Practices

General Security Measures

As general security measures, SICK recommends to minimize network exposure of the devices, restrict network access and follow recommended security practices in order to run the devices in a protected IT environment.

Vulnerability Classification

SICK performs vulnerability classification by using the CVSS scoring system (*CVSS v3.1*). The environmental score is dependent on the customer's environment and can affect the overall CVSS score. SICK recommends that customers individually evaluate the environmental score to achieve final scoring.

Resources

SICK PSIRT Security Advisories:
https://sick.com/psirt

SICK Operating Guidelines:
https://cdn.sick.com/media/docs/1/11/411/Special_information_CYBERSECURITY_BY_SICK_en_IM0084411.PDF

ICS-CERT recommended practices on Industrial Security:
http://ics-cert.us-cert.gov/content/recommended-practices

CVSS v3.1 Calculator:
https://www.first.org/cvss/calculator/3.1

Additional Product Information

SICK Package Analytics 4.0 up to 4.1.2	Product on sick.com: https://www.sick.com/de/de/p/p600146

History

Version	Release Date	Comment
1	2020-10-29	Initial Release
2	2023-02-09	Updated Advisory (only visual changes)