TLP:WHITE

SICK PSIRT
Security Advisory

Package Analytics affected by Windows TCP/IP vulnerability

Document ID:	SCA-2020-0005
Publication Date:	2020-10-29
CVSSv3 Base Score:	8.8 (CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C)
CVE Identifier:	CVE-2020-16898
Version:	V1.0

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.

AFFECTED PRODUCTS

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.

SOLUTION

This issue is addressed in the Microsoft update for CVE-2020-16898. It is available at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898

If you find yourself in a situation where an update is not doable. Microsoft advises the following workarounds:
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

Disable ICMPv6 RDNSS.

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.
General Security Practices
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.
Additional information on Industrial Security can be found at:
http://ics-cert.us-cert.gov/content/recommended-practices

Package Analytics has been verified to function without any issue and is compatible with the prescribed Microsoft update. No additional PA patches are necessary.

VULNERABILITY CLASSIFICATION

SICK performs vulnerability classification by using the CVSS scoring system (CVSS v3.0). 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]

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

HISTORY

Version	Release Date	Comment
V1	2020-10-29	Initial Release