

SICK PSIRT Security Advisory

MEAC AFFECTED BY WINDOWS SMBv1 VULNERABILITY

Document ID: SCA-2021-0002
Publication Date: 2021-08-09
CVSSv3 Base Score: 8.1 ([CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H](#))
[CVE Identifier] CVE-2017-0144
Version: V1.0

SUMMARY

Microsoft disclosed a critical security vulnerability in the Microsoft Server Message Block 1.0 (SMBv1) back in 2017. A successful exploitation of this vulnerability could lead to remote code execution with administrator privileges.

Since the MEAC central emission monitoring computer (EPC) has enabled the affected SMBv1 protocol to support older versions of external NAS drives, the devices are affected by this vulnerability. To reduce the overall attack surface, in addition to applying the windows remediation, we recommend disabling SMBv1 as backwards compatibility is no longer required.

AFFECTED PRODUCTS

Product	Sales Date	Remediation available
MEAC2012	All	Yes
MEAC300	Before December 2020	Yes

SOLUTION

This issue has been addressed in the Microsoft update for CVE-2017-0144. It is available at <https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-0144>.

We recommend disabling the SMBv1 protocol, as all current NAS drives support other protocols and there is no product-related reason to use it. Microsoft has published an article on [how to disable SMBv1](#). This will help to protect the system from exploits of this vulnerability.

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>

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-2017-0144>

Microsoft Guide to Disable SMBv1

<https://docs.microsoft.com/en-US/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3>

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	2021-08-09	Initial Release