TLP:WHITE

SICK PSIRT
Security Advisory

MEAC AFFECTED BY WINDOWS SMB3 VULNERABILITY

Document ID:	SCA-2020-0003
Publication Date:	2020-08-07
CVSSv3 Base Score:	10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
CVE Identifier:	CVE-2020-0796
Version:	V1.0

SUMMARY

Microsoft disclosed a critical vulnerability in the way Microsoft Server Message Block 3.1.1 (SMBv3) handles compressed connections. That may allow unauthenticated attackers to execute arbitrary code on a vulnerable device.
Since the MEAC central emission monitoring computer (EPC) acts as a SMB server to provide MEAC workstations with access to the filesystem in distributed MEAC-systems, the devices are affected by this vulnerability. Exploitation of this vulnerability could lead to remote code execution under login with administrator privileges.

AFFECTED PRODUCTS

All MEAC2012 or MEAC300 computers that equipped with Windows 10 Version 1903 or 1909 are affected, regardless if they are operated in a distributed MEAC-system or not, as the SMB ports are set to open during the setup of the computers.

SOLUTION

This issue has been addressed in the Microsoft update for CVE-2020-0796. It is available at https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-0796#ID0EGB.

Should this not be possible, we recommend following the workaround suggested by Microsoft and operate the MEAC in a protected networking environment. Blocking TCP port 445 at the perimeter firewall of the network segment will help to protect systems that are behind that firewall 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-2020-0796

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	2020-08-07	Initial Release