SICK
Sensor Intelligence.

TLP:WHITE

# SICK PSIRT
# Security Advisory

## MEAC affected by Windows SMBv3 vulnerability

| | |
|---|---|
| Document ID: | SCA-2020-0003 |
| Publication Date: | 2020-08-07 |
| CVE Identifier: | CVE-2020-0796 |
| CVSSv3 Base Score: | 10 |
| CVSSv3 Vector String: | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H |
| Version: | 2 |

## 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.

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.

## List of Products

| Product | Affected by |
|---|---|
| **SICK MEAC2012 with Microsoft Windows 10 Version 1903 & 1909** | CVE-2020-0796<br>Status: Known Affected<br>Remediation: Vendor fix, Mitigation |
| **SICK MEAC300 with Microsoft Windows 10 Version 1903 & 1909** | CVE-2020-0796<br>Status: Known Affected<br>Remediation: Vendor fix, Mitigation |

# Vulnerability Overview

## CVE-2020-0796

**CVE Description:** A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'.

**CVE-2020-0796** has been assigned to this vulnerability.
CVSSv3.1 base score: 10
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

**References:**
Microsoft Security Advisory:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796

# Remediations

## Vendor Fix for CVE-2020-0796

Details: This issue has been addressed in the Microsoft update for CVE-2020-0796.

URL: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv200005#ID0EUGAC

Valid for:

- SICK MEAC2012 with Microsoft Windows 10 Version 1903 & 1909
- SICK MEAC300 with Microsoft Windows 10 Version 1903 & 1909

## Mitigation for CVE-2020-0796

Details: Should Microsoft's remediation 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.

Valid for:

- SICK MEAC2012 with Microsoft Windows 10 Version 1903 & 1909
- SICK MEAC300 with Microsoft Windows 10 Version 1903 & 1909

# 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 MEAC300 with Microsoft Windows 10 Version 1903 & 1909** | Product on sick.com: https://www.sick.com/de/de/p/p475070 |

## History

| Version | Release Date | Comment |
|---|---|---|
| 1 | 2020-08-07 | Initial Release |
| 2 | 2023-02-09 | Updated Advisory (only visual changes) |