

# SICK PSIRT Security Advisory

## MEAC affected by Windows SMBv1 vulnerability

---

Document ID: SCA-2021-0002  
Publication Date: 2021-08-04  
CVE Identifier: CVE-2017-0144  
CVSSv3 Base Score: 8.1  
CVSSv3 Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H  
Version: 3

## 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.

## List of Products

---

Product	Affected by
<b>SICK MEAC2012</b>	<a href="#">CVE-2017-0144</a> Status: Known Affected Remediation: Vendor fix, Mitigation
<b>SICK MEAC300 with sales date before December 2020</b>	<a href="#">CVE-2017-0144</a> Status: Known Affected Remediation: Vendor fix, Mitigation

## Vulnerability Overview

---

### CVE-2017-0144 Improper Input Validation

**Summary:** Microsoft disclosed a critical security vulnerability in the Microsoft Server Message Block 1.0 (SMBv1) back in 2017.

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.

A successful exploitation of this vulnerability could lead to remote code execution with administrator privileges.

**CVE-2017-0144** has been assigned to this vulnerability.

CVSSv3.1 base score: 8.1

CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE identifier: CWE-20 (Improper Input Validation)

## Remediations

---

### Vendor Fix for CVE-2017-0144

Details: This issue has been addressed in the Microsoft update for CVE-2017-0144.

URL: <https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-0144>

Valid for:

- SICK MEAC2012
- SICK MEAC300 with sales date before December 2020

### Mitigation for CVE-2017-0144

Details: We recommend disabling the SMBv1 protocol, as all current NAS drives support other protocols. Microsoft has published an article on how to disable SMBv1. This will help to protect the system from exploits of this vulnerability.

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

Valid for:

- SICK MEAC2012
- SICK MEAC300 with sales date before December 2020

## 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://www.sick.com/media/docs/9/19/719/special\\_information\\_sick\\_operating\\_guidelines\\_cybersecurity\\_by\\_sick\\_en\\_im0106719.pdf](https://www.sick.com/media/docs/9/19/719/special_information_sick_operating_guidelines_cybersecurity_by_sick_en_im0106719.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 sales date  
before December 2020**

Product on sick.com: <https://www.sick.com/de/de/p/p475070>



Sensor Intelligence.

**TLP:WHITE**

## History

---

Version	Release Date	Comment
1	2021-08-04	Initial Release
2	2023-02-10	Updated Advisory (only visual changes)
3	2025-07-30	Updated Advisory: URL for SICK Operating Guidelines has been updated

**TLP:WHITE**