TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerabilities in SICK SOPAS ET

Document ID:	SCA-2021-0004
Publication Date:	2021-12-17
CVSSv3 Base Score:	8.6 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H)
[CVE Identifier:]	CVE-2021-32497, CVE-2021-32498, CVE-2021-32499
Version:	V1.0

SUMMARY

SICK received a report from Eden Bar of Claroty about multiple security vulnerabilities in the SICK SOPAS ET software.
An unauthorized attacker could potentially craft a malicious SOPAS Device Driver (SDD) file, that if a user imports that file to SOPAS ET could allow arbitrary code execution on the target system.
Currently SICK is not aware of any public exploits specifically targeting any of the vulnerabilities.
SICK has released a new version of the SICK SOPAS ET software and recommends updating to the newest version.

AFFECTED PRODUCTS

Product	Version	Remediation available
SICK SOPAS ET	Prior to version 2021.4 (4.8.0)	Yes

VULNERABILITY OVERVIEW

CVE-2021-32497 Inclusion of Functionality from Untrusted Control Sphere
SDD files might contain an executable file that will be listed as the Emulators inside SOPAS ET. When a user starts the emulator, the executable is run without further checks. Attackers could wrap any executable file into an SDD and provide this to a SOPAS ET user. When installing the SDD the user may not be aware about the executable inside of the SDD.

CVE-2021-32497 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.6
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

CVE-2021-32498 Improper Limitation of a Pathname to a Restricted Directory
When an SDD contains an emulator, the emulator location is part of the SDD manifest. Attackers could manipulate this location and use path traversal to target an arbitrary executable located on the host system. When the user starts the emulator from SOPAS ET, the corresponding executable will be started instead of the emulator.

CVE-2021-32498 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.6

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

CVE-2021-32499 Acceptance of Extraneous Untrusted Data With Trusted Data
The command line arguments that are passed to an emulator when starting it via SOPAS ET, are part of the SDD manifest. Attackers could manipulate the arguments to pass in any value to the executable. In combination with CVE-2021-32498 the attacker could target an arbitrary executable with any arguments on the host system.

CVE-2021-32499 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.6
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

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.x). 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

HISTORY

Version	Release Date	Comment
V1	2021-12-17	Initial Release