SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerabilities in SICK Package Analytics

Document ID:	SCA-2020-0002
Publication Date:	2020-07-28
CVE Identifiers:	CVE-2020-2076, CVE-2020-2077, CVE-2020-2078
Version:	2

Summary

SICK received a report about multiple security vulnerabilities in the Package Analytics software. Successful exploitation of these vulnerabilities could allow an unauthorized remote attacker to read and write the configuration of the software, read data directly from the file system and view passwords in plain text. Currently SICK is not aware of any public exploits specifically targeting any of the vulnerabilities.
SICK has released a new version of the SICK Package Analytics software and recommends updating to the newest version.

List of Products

Product	Affected by
SICK Package Analytics 4.0.0	CVE-2020-2076 Status: Known Affected Remediation: Vendor fix, Workaround
	CVE-2020-2077 Status: Known Affected Remediation: Vendor fix, Workaround
SICK Package Analytics 4.1.1	CVE-2020-2078 Status: Known Affected Remediation: Vendor fix, Workaround

Vulnerability Overview

CVE-2020-2076 Authentication Bypass Using an Alternate Path or Channel

CVE description: The affected product is vulnerable to an authentication bypass by directly interfacing with the REST API. An attacker can send unauthorized requests, bypass current authentication controls presented by the application and could potentially write files without authentication.

CVE-2020-2076 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.1
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:H/RL:U/RC:C/CR:H
CWE identifier: CWE-288 (Authentication Bypass Using an Alternate Path or Channel)

CVE-2020-2077 Incorrect Default Permissions

CVE description: The affected product is vulnerable due to incorrect default permissions settings. An unauthorized attacker could read sensitive data from the system by querying for known files using the REST API directly.

CVE-2020-2077 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.6
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:H/RL:U/RC:C/CR:H
CWE identifier: CWE-276 (Incorrect Default Permissions)

CVE-2020-2078 Cleartext Storage of Sensitive Information

CVE description: Passwords are stored in plain text within the configuration of the software. An authorized attacker could access these stored plaintext credentials and gain access to the ftp service. Storing a password in plaintext allows attackers to easily gain access to systems, potentially compromising personal information or other sensitive information.

CVE-2020-2078 has been assigned to this vulnerability.
CVSSv3.1 base score: 6.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:H/RL:U/RC:C/CR:H
CWE identifier: CWE-312 (Cleartext Storage of Sensitive Information)

Remediations

Vendor Fix for CVE-2020-2076

Details: Update to Package Analytics 4.1.1 or 4.1.2

Valid for:

- SICK Package Analytics 4.0.0

Workaround for CVE-2020-2076

Details: Restrict access to the device to the internal or VPN network and to trusted IP addresses only.

Valid for:

- SICK Package Analytics 4.0.0

Vendor Fix for CVE-2020-2077

Details: Update to Package Analytics 4.1.1 or 4.1.2

Valid for:

- SICK Package Analytics 4.0.0

Workaround for CVE-2020-2077

Details: Restrict access to the device to the internal or VPN network and to trusted IP addresses only.

Valid for:

- SICK Package Analytics 4.0.0

Vendor Fix for CVE-2020-2078

Details: Update to Package Analytics 4.1.2

Valid for:

- SICK Package Analytics 4.1.1

Workaround for CVE-2020-2078

Details: Restrict access to the device to the internal or VPN network and to trusted IP addresses only.

Valid for:

- SICK Package Analytics 4.1.1

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 Package Analytics 4.0.0	Product on sick.com: https://www.sick.com/de/de/p/p600146
SICK Package Analytics 4.1.1	Product on sick.com: https://www.sick.com/de/de/p/p600146

History

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