TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerabilities in SICK Package Analytics

Document ID: SCA-2020-0002
Publication Date: 28.07.2020
CVSSv3 Base Score: 9.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:H/RL:U/RC:C/CR:H)
CVE Identifier: CVE-2020-2076, CVE-2020-2077, CVE-2020-2078
Version: V1.0

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.

AFFECTED PRODUCTS

Product	Version	Affected by	Remediation
SICK Package Analytics	V04.0.0	CVE-2020-2076 CVE-2020-2077	Update to version V04.1.1 or newer
SICK Package Analytics	V04.1.1	CVE-2020-2078	Update to version V04.1.2

Vulnerability Overview

CVE-2020-2076 - Authentication Bypass Using an Alternate Path or Channel (CWE-288)
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.
CVSS v3 base score: 9.1
CVSS v3 vector string: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:H/RL:U/RC:C/CR:H

CVE-2020-2077 - Incorrect Default Permissions (CWE-276)
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.
CVSS v3 base score: 8.6
CVSS v3 vector string: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:H/RL:U/RC:C/CR:H

TLP:WHITE

CVE-2020-2078 - Cleartext Storage of Sensitive Information (CWE-312)
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.
CVSS v3 base score: 6.3
CVSS v3 vector string: AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:H/RL:U/RC:C/CR:H

WORKAROUNDS AND MITIGATIONS

The recommended measure for the above noted vulnerabilities is to update Package Analytics to the appropriate version. Specifically, for issues – CVE-2020-2076 and CVE-2020-2077, the recommended fix is to update to Package Analytics 4.1.1 or 4.1.2. For issue – CVE-2020-2078, the recommended fix is to update to Package Analytics 4.1.2.

In general, we recommend updating to version 4.1.2 to resolve all three observed issues.

SICK recommends the following measure for solutions where an update is not applicable or a technical fix is not available:

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

GENERAL SECURITY RECOMMENDATIONS

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:
https://sick.com/psirt

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.

TLP:WHITE

RESOURCES

CVSS Calculator
https://www.first.org/cvss/calculator/3.0#

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
V1.0	28.07.2020	Initial Release