Several vulnerabilities affecting the Cosy+ product line

HMSSAR-2024-07-29-001

Version	Summary of changes	Date
1	Initial release	2024-07-29
2	Typo	2024-08-07

Overview

An independent researcher has discovered several vulnerabilities affecting the Cosy+ product line.

CVE-2024-33892, CVE-2024-33896, CVE-2024-33893, CVE-2024-33895, CVE-2024-33894, CVE-2024-33897

Affected products and versions

All Cosy+ versions running a firmware version 21.x below 21.2s10 or a firmware version 22.x below 22.1s3.

CVE-2024-33892

Impact

Cosy+ devices running a firmware 21.x below 21.2s10 or a firmware 22.x below 22.1s3 are susceptible to information leakage through cookies.

Severity / CVSS Score

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/S:N/AU:N/R:U/RE:M/U:Red
CVSS4 scoring: 7.4 (high)

Recommendations

HMS Networks recommends upgrading your Cosy+ devices to firmware versions >= 21.2s10 or 22.1s3.

CVE-2024-33896

Impact

Cosy+ devices running a firmware 21.x below 21.2s10 or a firmware 22.x below 22.1s3 are vulnerable to code injection due to improper parameter blacklisting.

Severity / CVSS Score

CVSS:4.0/AV:A/AC:L/AT:N/PR:H/UI:A/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/S:N/AU:N/R:U/RE:M/U:Red

CVSS4 scoring: 3.3 (low)

Recommendations

HMS Networks recommends upgrading your Cosy+ devices to firmware versions >= 21.2s10 or 22.1s3.

CVE-2024-33893

Impact

Cosy+ devices running a firmware 21.x below 21.2s10 or a firmware 22.x below 22.1s3 are vulnerable to XSS when displaying the logs due to improper input sanitization.

Severity / CVSS Score

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/S:N/AU:Y/R:U/RE:M/U:Red

CVSS4 scoring: 2.1 (low)

Recommendations

HMS Networks recommends upgrading your Cosy+ devices to firmware versions >= 21.2s10 or 22.1s3.

CVE-2024-33895

Impact

Cosy+ devices running a firmware 21.x below 21.2s10 or a firmware 22.x below 22.1s3 use a unique key to encrypt the configuration parameters.

This is fixed in version 21.2s10 and 22.1s3, the key is now unique per device.

Severity / CVSS Score

CVSS:4.0/AV:P/AC:H/AT:P/PR:H/UI:A/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N

CVSS4 scoring: 4.4 (medium)

Recommendations

HMS Networks recommends upgrading your Cosy+ devices to firmware versions >= 21.2s10 or 22.1s3.

CVE-2024-33894

Description

Cosy+ devices running a firmware 21.x below 21.2s10 or a firmware 22.x below 22.1s3 are executing several processes with elevated privileges.

However, there is no impact for the user or the device

Severity / CVSS Score

CVSS:4.0/AV:A/AC:H/AT:P/PR:H/UI:A/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N

CVSS4 scoring: 1.0 (low)

Recommendations

This is not an issue. However, HMS Networks recommends upgrading your Cosy+ devices.

CVE-2024-33897

Impact

A compromised Cosy+ device could be used to request a Certificate Signing Request from Talk2m for another device, resulting in an availability issue.

Recommendations

The issue was patched on the Talk2m production server on April 18, 2024.

Acknowledgements

HMS thanks Moritz Abrell from SySS for finding and disclosing the above vulnerabilities collaboratively and responsibly.