SSA-225840: Vulnerabilities in the Network Communication Stack in Sinteso EN and Cerberus PRO EN Fire Protection Systems

Publication Date: 2024-03-12
Last Update: 2024-03-12
Current Version: V1.0
CVSS v3.1 Base Score: 10.0
CVSS v4.0 Base Score: 10.0

SUMMARY

Several products used in Sinteso EN and Cerberus PRO EN Fire Protection Systems contain buffer overflow vulnerabilities in the network communication stack. Successful exploitation of the vulnerabilities could allow an unauthenticated attacker, who gained access to the fire protection system network, to execute arbitrary code on the affected products (CVE-2024-22039) or create a denial of service condition (CVE-2024-22040, CVE-2024-22041).

Product-specific impact of the individual vulnerabilities is documented in the chapter “Vulnerability Description”.

Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Cerberus PRO EN Engineering Tool: All versions < IP8 affected by CVE-2024-22039	Update to IP8 or later version
Cerberus PRO EN Engineering Tool: All versions affected by CVE-2024-22040, CVE-2024-22041	Currently no fix is available
Cerberus PRO EN Fire Panel FC72x: All versions < IP8 affected by CVE-2024-22039	Update to IP8 or later version
Cerberus PRO EN Fire Panel FC72x: All versions < IP8 SR4 affected by CVE-2024-22040, CVE-2024-22041	Update to IP8 SR4 or later version
Cerberus PRO EN X200 Cloud Distribution: All versions < V4.0.5016 affected by CVE-2024-22039	Update to V4.0.5016 or later version
Cerberus PRO EN X200 Cloud Distribution: All versions < V4.3.5618 affected by CVE-2024-22040, CVE-2024-22041	Update to V4.3.5618 or later version
Cerberus PRO EN X300 Cloud Distribution: All versions < V4.2.5015 affected by CVE-2024-22039	Update to V4.2.5015 or later version
Cerberus PRO EN X300 Cloud Distribution: All versions < V4.3.5617 affected by CVE-2024-22040, CVE-2024-22041	Update to V4.3.5617 or later version

Sinteso FS20 EN Engineering Tool: All versions < MP8 affected by CVE-2024-22039	Update to MP8 or later version
Sinteso FS20 EN Engineering Tool: All versions affected by CVE-2024-22040, CVE-2024-22041	Currently no fix is available
Sinteso FS20 EN Fire Panel FC20: All versions < MP8 affected by CVE-2024-22039	Update to MP8 or later version
Sinteso FS20 EN Fire Panel FC20: All versions < MP8 SR4 affected by CVE-2024-22040, CVE-2024-22041	Update to MP8 SR4 or later version
Sinteso FS20 EN X200 Cloud Distribution: All versions < V4.0.5016 affected by CVE-2024-22039	Update to V4.0.5016 or later version
Sinteso FS20 EN X200 Cloud Distribution: All versions < V4.3.5618 affected by CVE-2024-22040, CVE-2024-22041	Update to V4.3.5618 or later version
Sinteso FS20 EN X300 Cloud Distribution: All versions < V4.2.5015 affected by CVE-2024-22039	Update to V4.2.5015 or later version
Sinteso FS20 EN X300 Cloud Distribution: All versions < V4.3.5617 affected by CVE-2024-22040, CVE-2024-22041	Update to V4.3.5617 or later version
Sinteso Mobile: All versions < V3.0.0 affected by CVE-2024-22039	Update to V3.0.0 or later version https://play.google.com/store/apps/details?id=com.siemens.fsp.f20.smartphone.sinteso
Sinteso Mobile: All versions affected by CVE-2024-22040, CVE-2024-22041	Currently no fix is planned

WORKAROUNDS AND MITIGATIONS

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure Siemens strongly recommends to protect network access to affected products with appropriate mechanisms. It is advised to follow recommended security practices in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

Cerberus PRO EN is a fire protection system consisting of fire panels, detection and management stations. It is available for Siemens Partners and complies with the European standard EN 54 for fire detection and alarm systems.

Sinteso EN is a fire protection system consisting of fire panels, detection and management stations. It complies with the European standard EN 54 for fire detection and alarm systems.

Sinteso Mobile is the mobile app for remote access to Sinteso / Cerberus PRO EN fire protection systems.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2024-22039

The network communication library in affected systems does not validate the length of certain X.509 certificate attributes which might result in a stack-based buffer overflow. This could allow an unauthenticated remote attacker to execute code on the underlying operating system with root privileges.

CVSS v3.1 Base Score	10.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	10.0
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Product Specific Vulnerability Description

For the following products, the impact of the vulnerability is different.

Cerberus PRO EN Engineering Tool:

Successful exploitation requires an on-path attacker that intercepts the communication of the engineering tool in the fire system network; code execution might be possible on the underlying operating system with the privileges of the engineering tool user account.

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H (9.0)
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H (9.0)

Sinteso FS20 EN Engineering Tool:

Successful exploitation requires an on-path attacker that intercepts the communication of the engineering tool in the fire system network; code execution might be possible on the underlying operating system with the privileges of the engineering tool user account.

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H (9.0)
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H (9.0)

Sinteso Mobile:

Successful exploitation requires an on-path attacker that intercepts the communication of the app in the fire system network; possible impact is limited to the app, not the underlying operating system.

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H (8.1)
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N (7.7)

Vulnerability CVE-2024-22040

The network communication library in affected systems insufficiently validates HMAC values which might result in a buffer overread. This could allow an unauthenticated remote attacker to crash the network service.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-125: Out-of-bounds Read

Product Specific Vulnerability Description

For the following products, the impact of the vulnerability is different.

Cerberus PRO EN Engineering Tool:

Successful exploitation requires an on-path attacker that intercepts the communication of the engineering tool in the fire system network; possible impact is limited to the tool, not the underlying operating system.

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H (5.9)
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N (6.0)

Sinteso FS20 EN Engineering Tool:

Successful exploitation requires an on-path attacker that intercepts the communication of the engineering tool in the fire system network; possible impact is limited to the tool, not the underlying operating system.

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H (5.9)
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N (6.0)

Sinteso Mobile:

Successful exploitation requires an on-path attacker that intercepts the communication of the app in the fire system network; possible impact is limited to the app, not the underlying operating system.

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H (5.9)
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N (6.0)

Vulnerability CVE-2024-22041

The network communication library in affected systems improperly handles memory buffers when parsing X.509 certificates. This could allow an unauthenticated remote attacker to crash the network service.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Product Specific Vulnerability Description

For the following products, the impact of the vulnerability is different.

Cerberus PRO EN Engineering Tool:

Successful exploitation requires an on-path attacker that intercepts the communication of the engineering tool in the fire system network; possible impact is limited to the tool, not the underlying operating system.

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H (5.9)
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N (6.0)

Sinteso FS20 EN Engineering Tool:

Successful exploitation requires an on-path attacker that intercepts the communication of the engineering tool in the fire system network; possible impact is limited to the tool, not the underlying operating system.

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H (5.9)
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N (6.0)

Sinteso Mobile:

Successful exploitation requires an on-path attacker that intercepts the communication of the app in the fire system network; possible impact is limited to the app, not the underlying operating system.

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H (5.9)
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N (6.0)

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2024-03-12): Publication Date

TERMS OF USE