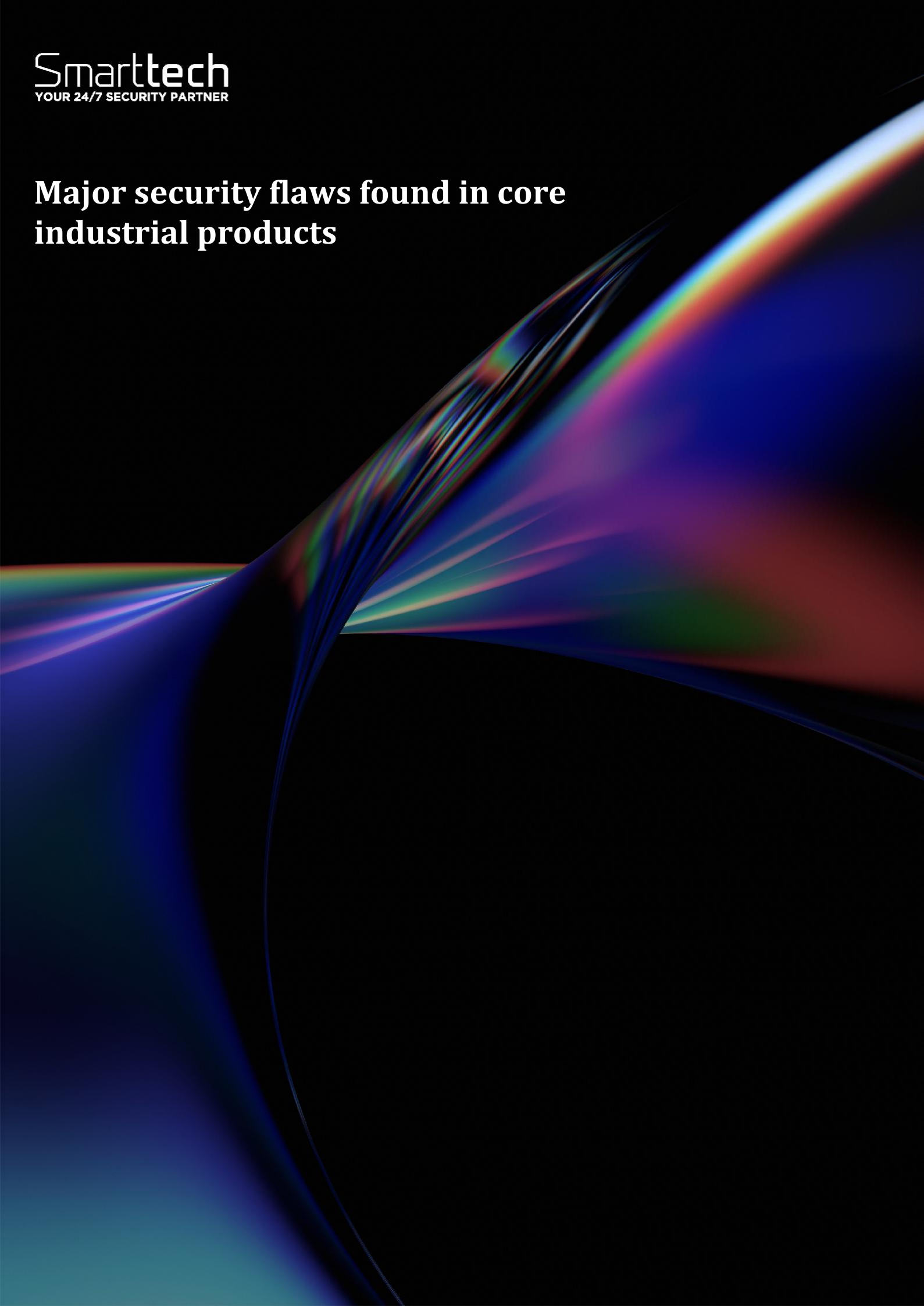
Smarttech
YOUR 24/7 SECURITY PARTNER

Major security flaws found in core industrial products



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	25
Authors	Alex Ciuta < alexandru.ciuta@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-02-18
Issue Date	2026-02-18

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

Multiple vulnerabilities have been identified in the following products: Honeywell CCTV Products, GE Vernova Enervista UR Setup, Delta Electronics ASDA-Soft, and Siemens Simcenter Femap and Nastran. Successful exploitation could lead to account takeovers, unauthorized access to camera feeds, manipulation of recovery email settings, code execution with elevated privileges, corruption of structured exception handlers through out-of-bounds writes, and application crashes or arbitrary code execution triggered by malicious NDB or XDB files. These issues collectively pose risks to system integrity, confidentiality, and operational availability.

Honeywell CCTV Products

Summary

Successful exploitation of this vulnerability could lead to account takeovers and unauthorized access to camera feeds; an unauthenticated attacker may change the recovery email address, potentially leading to further network compromise.

The following versions of Honeywell CCTV Products are affected:

- I-HIB2PI-UL 2MP IP 6.1.22.1216 (CVE-2026-1670)
- SMB NDAA MVO-3 WDR_2MP_32M_PTZ_v2.0 (CVE-2026-1670)
- PTZ WDR 2MP 32M WDR_2MP_32M_PTZ_v2.0 (CVE-2026-1670)
- 25M IPC WDR_2MP_32M_PTZ_v2.0 (CVE-2026-1670)

CVSS: v3 9.8
Vendor: Honeywell
Equipment: Honeywell CCTV Products
Vulnerabilities: Missing Authentication for Critical Function

Vulnerabilities

CVE ID	Base Severity	Base Score	Description
CVE-2026-1670	Critical	9.8	The affected product is vulnerable to an unauthenticated API endpoint exposure, which may allow an attacker to remotely change the "forgot password" recovery email address.

Remediations

- Honeywell recommends users contact Honeywell at https://www.honeywell.com/us/en/contact/support for patch information.

GE Vernova Enervista UR Setup

Summary

Successful exploitation of these vulnerabilities may allow code execution with elevated privileges.

The following versions of GE Vernova Enervista UR Setup are affected:

- Enervista UR Setup <8.70 (CVE-2026-1762, CVE-2026-1763)

CVSS: v3 7.8
Vendor: GE Vernova
Equipment: GE Vernova Enervista UR Setup
Vulnerabilities: Uncontrolled Search Path Element, Path Traversal: '.../...//'

Vulnerabilities

CVE ID	Base Severity	Base Score	Description
CVE-2026-1763	High	7.8	The GE Vernova Enervista UR Setup Installer for versions prior to 8.70 are vulnerable to DLL hijacking. When running the installer in a location with unknown or untrusted DLLs, an attacker could obtain code execution with administrative privileges.
CVE-2026-1763	Low	3.3	GE Vernova Enervista UR Setup versions prior to 8.70 are vulnerable to directory traversal when opening certain firmware update files. This could allow an attacker to write to some files on the filesystem with the privileges of the logged-in user.

Remediations

- GE Vernova recommends affected users to use patched versions of Enervista UR Setup: Versions 8.70 or later.

Delta Electronics ASDA-Soft

Summary

Successful exploitation of this vulnerability may allow an attacker to write arbitrary data beyond the bounds of a stack-allocated buffer, leading to the corruption of a structured exception handler (SEH).

The following versions of Delta Electronics ASDA-Soft are affected:

- ASDA-Soft <=7.2.0.0 (CVE-2026-1361)

CVSS: v3 7.8
Vendor: Delta Electronics
Equipment: Delta Electronics ASDA-Soft
Vulnerabilities: Stack-based Buffer Overflow

Vulnerabilities

CVE ID	Base Severity	Base Score	Description
CVE-2026-1361	High	7.8	A stack-based buffer overflow vulnerability exists in ASDA_Soft version 7.2.0.0 when parsing .par files. The root cause is the improper validation of a user-controlled size parameter, which is checked incorrectly against the upper limits of the local buffer. This allows data to be written past the end of the buffer.

Remediations

- Delta has fixed this vulnerability and released a new version v7.2.2.0 at Delta Download Center

Siemens Simcenter Femap and Nastran

Summary

Siemens Simcenter Femap and Nastran is affected by multiple file parsing vulnerabilities that could be triggered when the application reads files in NDB and XDB formats. If a user is tricked to open a malicious file with any of the affected products, this could lead the application to crash or potentially lead to arbitrary code execution. Siemens has released new versions for the affected products and recommends to update to the latest versions.

The following versions of Siemens Simcenter Femap and Nastran are affected:

- Simcenter Femap vers:intdot/<2512 (CVE-2026-23715, CVE-2026-23716, CVE-2026-23717, CVE-2026-23718, CVE-2026-23719, CVE-2026-23720)
- Simcenter Nastran vers:intdot/<2512 (CVE-2026-23715, CVE-2026-23716, CVE-2026-23717, CVE-2026-23718, CVE-2026-23719, CVE-2026-23720)

CVSS: v3 7.8
Vendor: Siemens
Equipment: Siemens Simcenter Femap and Nastran
Vulnerabilities: Out-of-bounds Write, Out-of-bounds Read, Heap-based Buffer Overflow

Vulnerabilities

CVE ID	Base Severity	Base Score	Description
CVE-2026-23715	High	7.8	The affected applications contains an out of bounds write vulnerability while parsing specially crafted XDB files. This could allow an attacker to execute code in the context of the current process.
CVE-2026-23716	High	7.8	The affected applications contains an out of bounds read vulnerability while parsing specially crafted XDB files. This could allow an attacker to execute code in the context of the current process.
CVE-2026-23717	High	7.8	The affected applications contains an out of bounds read vulnerability while parsing specially crafted XDB files. This could allow an attacker to execute code in the context of the current process.
CVE-2026-23718	High	7.8	The affected applications contains an out of bounds read vulnerability while parsing specially crafted NDB files. This could allow an attacker to execute code in the context of the current process.
CVE-2026-23719	High	7.8	The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted NDB files. This could allow an attacker to execute code in the context of the current process.
CVE-2026-23720	High	7.8	The affected applications contains an out of bounds read vulnerability while parsing specially crafted NDB files. This could allow an attacker to execute code in the context of the current process.

Remediations

- Do not open untrusted XDB files in affected applications
- Do not open untrusted NDB files in affected applications

References

https://www.cisa.gov/news-events/ics-advisories/icsa-26-048-01
https://www.cisa.gov/news-events/ics-advisories/icsa-26-048-02
https://www.cisa.gov/news-events/ics-advisories/icsa-26-048-03
https://www.cisa.gov/news-events/ics-advisories/icsa-26-048-04

CVEs

CVE-2026-1670,
CVE-2026-1762,
CVE-2026-1763,
CVE-2026-1361,
CVE-2026-23715,
CVE-2026-23716,
CVE-2026-23717,
CVE-2026-23718,
CVE-2026-23719,
CVE-2026-23720

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com