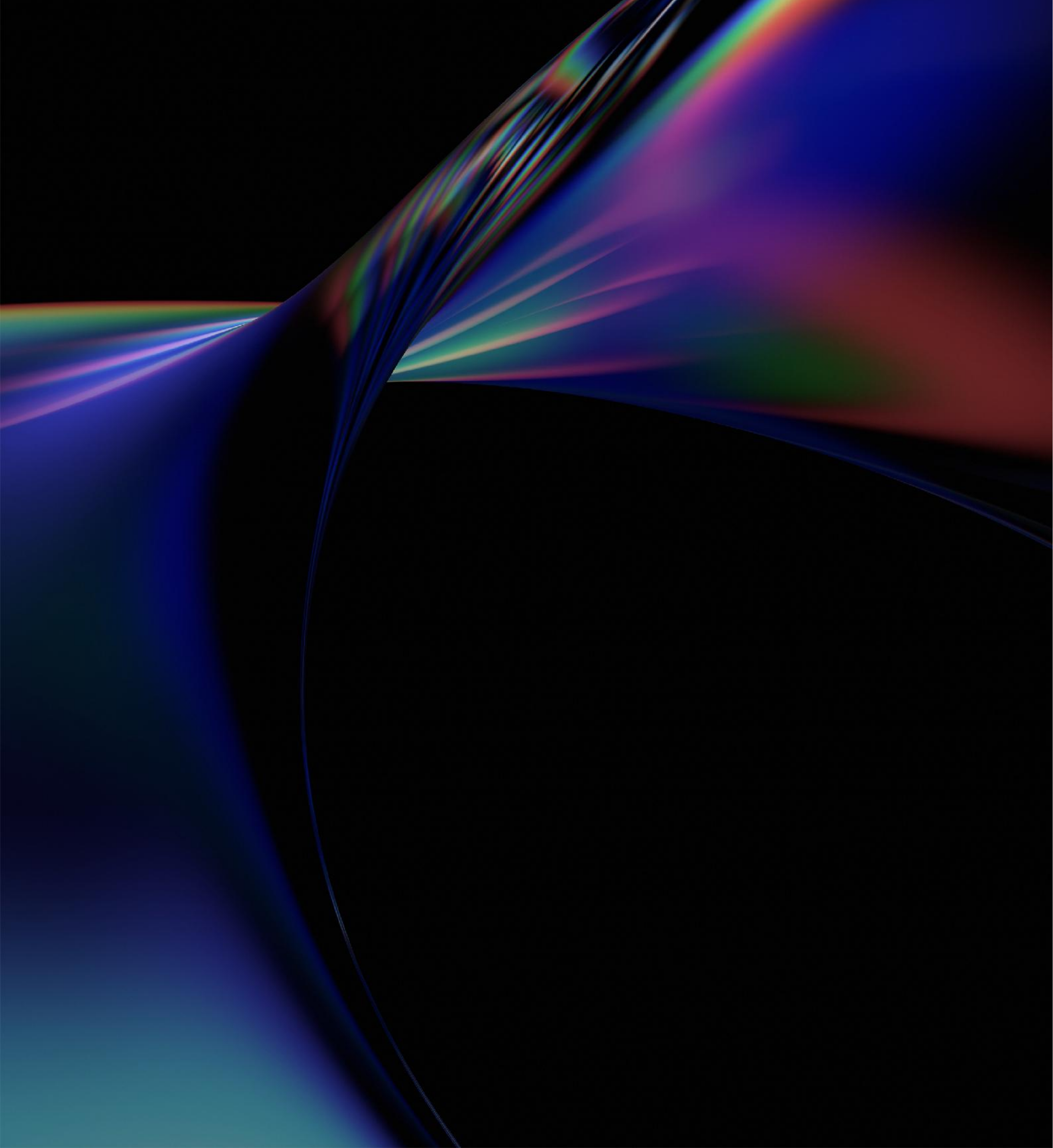
Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Vulnerabilities in Industrial Control Systems - 11th February 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	20
Authors	Ana Nastase< ana.nastase@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-02-11
Issue Date	2026-02-10

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 ICS-connected and medical products: Yokogawa FAST/TOOLS, ZLAN Information Technology ZLAN5143D, AVEVA PI Data Archive, AVEVA PI to CONNECT Agent, and the ZOLL ePCR iOS Mobile Application. Successful exploitation could lead to authentication bypass, unauthorized access to industrial or medical data, denial-of-service conditions, compromise of system availability and integrity, unauthorized configuration changes, and exposure of sensitive operational or protected health information.

Yokogawa FAST/TOOLS

Summary

- Successful exploitation of these vulnerabilities could allow an attacker to redirected users to malicious sites, decrypt communications, perform a man-in-the-middle (MITM) attack, execute malicious scripts, steal files, and perform other various attacks.
- The following versions of Yokogawa FAST/TOOLS are affected: **FAST/TOOLS >=R9.01|<=R10.04**
- **CVSS v.3 8.2**
- **Vendor:** Yokogawa
- **Equipment:** Yokogawa FAST/TOOLS
- **Vulnerabilities:** Generation of Error Message Containing Sensitive Information, Cross-Site Request Forgery (CSRF), Use of a Broken or Risky Cryptographic Algorithm, Exposure of Sensitive System Information to an Unauthorized Control Sphere, Improperly Implemented Security Check for Standard, Reliance on IP Address for Authentication, Cleartext Transmission of Sensitive Information, Exposure of Private Personal Information to an Unauthorized Actor, Improper Neutralization of Invalid Characters in Identifiers in Web Pages, Path Traversal: '\..\filename'

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2025-66594	Medium	Detailed messages are displayed on the error page. This information could be exploited by an attacker for other attacks.
CVE-2025-66595	Medium	This product is vulnerable to cross-site request forgery (CSRF). When a user accesses a link crafted by an attacker, the user's account could be compromised.
CVE-2025-66597	High	This product supports weak cryptographic algorithms, potentially allowing an attacker to decrypt communications with the web server.
CVE-2025-66598	High	This product supports old SSL/TLS versions, potentially allowing an attacker to decrypt communications with the web server.
CVE-2025-66599	Medium	Physical paths could be displayed on web pages. This information could be exploited by an attacker for other attacks.

CVE-2025-66600	High	This product lacks HSTS (HTTP Strict Transport Security) configuration. When an attacker performs a Man in the middle (MITM) attack, communications with the web server could be sniffed.
CVE-2025-66601	Medium	This product does not specify MIME types. When an attacker performs a content sniffing attack, malicious scripts could be executed.
CVE-2025-66602	Medium	The web server accepts access by IP address. When a worm that randomly searches for IP addresses intrudes into the network, it could potentially be attacked by the worm.
CVE-2025-66603	Low	The web server accepts the OPTIONS method. An attacker could potentially use this information to carry out other attacks.
CVE-2025-66604	Low	The library version could be displayed on the web page. This information could be exploited by an attacker for other attacks.
CVE-2025-66605	Low	Since there are input fields on this web page with the autocomplete attribute enabled, the input content could be saved in the browser the user is using.
CVE-2025-66606	Low	This product does not properly encode URLs. An attacker could tamper with web pages or execute malicious scripts.
CVE-2025-66607	Low	The response header contains an insecure setting. Users could be redirected to malicious sites by an attacker.
CVE-2025-66608	High	This product fails to adequately validate URLs. An attacker could send maliciously crafted requests to gain unauthorized access to files on the web server.

Remediations

- Yokogawa recommends users update to revision R10.04 and apply patch software (CS_e12787). After the patch is applied, users should apply R10.04 SP3.
- Yokogawa strongly recommends that all users establish and maintain a comprehensive security program, not just for addressing the vulnerability identified in this YSAR. Security program components include patch updates, antivirus software, backup and recovery solutions, zoning, hardening, whitelisting, firewalls, and other related measures. Yokogawa can assist organizations in setting up and continuously maintaining a security program. As a starting point for developing the most effective risk mitigation plan, Yokogawa offers security risk assessment services.

ZLAN Information Technology Co. ZLAN5143D

Summary

- Successful exploitation of these vulnerabilities could result in an attacker bypassing authentication or resetting the device password.
- The following versions of ZLAN Information Technology Co. ZLAN5143D are affected: **ZLAN5143D v1.600**
- **CVSS v3 9.8**
- **Vendor:** ZLAN Information Technology Co.
- **Equipment:** ZLAN Information Technology Co. ZLAN5143D
- **Vulnerabilities:** Missing Authentication for Critical Function

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-25084	Critical	Authentication for the device can be bypassed by directly accessing internal URLs.
CVE-2026-24789	Critical	An unprotected API endpoint allows an attacker to remotely change the device password without providing authentication.

Remediations

ZLAN Information Technology Co. did not respond to CISA's attempts at coordination. Users of ZLAN5143D devices are encouraged to contact ZLAN and keep their systems up to date.

AVEVA PI Data Archive

Summary

- Successful exploitation of this vulnerability could result in a denial-of-service condition.
- The following versions of AVEVA PI Data Archive are affected: **PI Data Archive PI Server <=2018_SP3_Patch_7, PI Data Archive PI Server 2023, PI Data Archive PI Server 2023_Patch_1, PI Data Archive PI Server 2024**
- **CVSS v3 7.5**
- **Vendor:** AVEVA
- **Equipment:** AVEVA PI Data Archive
- **Vulnerabilities:** Uncaught Exception

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-1507	High	The affected products are vulnerable to an uncaught exception that could allow an unauthenticated attacker to remotely crash core PI services resulting in a denial of service.

Remediations

- AVEVA recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation. Users of affected product versions should apply security updates to mitigate the risk of exploit.
- All impacted versions of PI Data Archive can be fixed by upgrading to PI Server 2024 R2 or later.
- PI Data Archive delivered by PI Server 2018 SP3 Patch 7 and prior can be fixed by upgrading to PI Server 2018 SP3 Patch 8 or higher
- The following general defensive measures are recommended:
  -Monitor liveness of services listed in your installation's "\PI\adm\pisrvstart.bat".
  -Set the PI Data Archive Subsystem services to automatically restart.
  -PI Data Archive nodes should limit port 5450 inbound access to trusted workstations, users, and software.

AVEVA PI to CONNECT Agent

Summary

- Successful exploitation of this vulnerability could result in unauthorized access to the proxy server.
- The following versions of AVEVA PI to CONNECT Agent are affected: **PI to CONNECT Agent <=v2.4.2520**
- **CVSS v3 6.5**
- **Vendor:** AVEVA
- **Equipment:** AVEVA PI to CONNECT Agent
- **Vulnerabilities:** Insertion of Sensitive Information into Log File

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-1495	Medium	The vulnerability, if exploited, could allow an attacker with Event Log Reader (S-1-5-32-573) privileges to obtain proxy details, including URL and proxy credentials, from the PI to CONNECT event log files. This could enable unauthorized access to the proxy server.

Remediations

- AVEVA recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.
- Users of affected product versions should apply security updates to mitigate the risk of proxy details exposure in newly generated PI to CONNECT Agent event logs.
- Users who have used affected product versions, should review existing PI to CONNECT Agent event logs (live/backups/copies) for exposed proxy connection details and consider purging the sensitive data from logs and/or configuring new credentials for access to the proxy service.
- The following general defensive measures are recommended:

-Remove use of plain text passwords in proxy URLs. Alternatively, if passwords are required by the proxy, then use least-privilege credentials.
-Ensure only trusted users are given Event Log Reader (S-1-5-32-573) privileges on hosts where PI to CONNECT is installed.
-Review existing PI to CONNECT event logs (live/backups/copies) for exposed proxy connection details and consider purging the sensitive data from logs and/or configuring new credentials for access to the proxy service.
-All affected versions can be fixed by upgrading to PI to CONNECT Agent v2.5.2790 or higher.

ZOLL ePCR IOS Mobile Application

Summary

- Successful exploitation of this vulnerability could allow an attacker to gain unauthorized access to protected health information (PHI) or device telemetry.
- The following versions of ZOLL ePCR IOS Mobile Application are affected**: ePCR IOS Mobile Application 2.6.7**
- **CVSS v3 5.5**
- **Vendor:** ZOLL
- **Equipment:** ZOLL ePCR IOS Mobile Application
- **Vulnerabilities:** Insertion of Sensitive Information into Externally-Accessible File or Directory

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2025-12699	Medium	The ZOLL ePCR IOS application reflects unsanitized user input into a WebView. Attacker-controlled strings placed into PCR fields (run number, incident, call sign, notes) are interpreted as HTML/JS when the app prints or renders that content. In the proof of concept (POC), injected scripts return local file content, which would allow arbitrary local file reads from the app's runtime context. These local files contain device and user data within the ePCR medical application, and if exposed, would allow an attacker to access protected health information (PHI) or device telemetry.

Remediations

ZOLL ePCR IOS application was decommissioned in May 2025. ZOLL has no current plans to provide a replacement application. If users have questions or concerns, they are encouraged to reach out directly to ZOLL Support.

References

https://www.cisa.gov/news-events/ics-advisories/icsa-26-041-01
https://www.cisa.gov/news-events/ics-advisories/icsa-26-041-02
https://www.cisa.gov/news-events/ics-advisories/icsa-26-041-03
https://www.cisa.gov/news-events/ics-advisories/icsa-26-041-04
https://www.cisa.gov/news-events/ics-medical-advisories/icsma-26-041-01

CVEs

CVE-2025-66594,
CVE-2025-66595,
CVE-2025-66597,
CVE-2025-66598,
CVE-2025-66599,
CVE-2025-66600,
CVE-2025-66601,
CVE-2025-66602,
CVE-2025-66603,
CVE-2025-66604,
CVE-2025-66605,
CVE-2025-66606,
CVE-2025-66607,
CVE-2025-66608,
CVE-2026-25084,
CVE-2026-24789,
CVE-2026-1507,
CVE-2026-1495,
CVE-2025-12699

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com