DOCUMENT ID: SA26P003
VERSION: 1.0
DATE: 2026-11-09

CYBER SECURITY ADVISORY

OpenSSL Vulnerabilities in B&R products

CVE ID: CVE-2025-15467, CVE-2025-11187

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by B&R.

B&R provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall B&R or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if B&R or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from B&R, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Purpose

B&R has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, B&R immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations.

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If B&R is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of B&R's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

Affected products

B&R advises its customers to analyze whether their product configuration may be affected by the vulnerabilities based on the aspects listed in the "Vulnerability severity and details" section.

Product	Affected versions
mapp View	<6.6.0
Automation Runtime	Not vulnerable
B&R Live Utils	<3.0.2
B&R Linux 12	<1.1.1
PPC80	<1.8.2
PPT50	<1.8.0
PPC50	<1.8.0
PPT80	<1.8.2
PFT51	<1.8.2
PFT50	<1.8.0
PPT30	<1.8.0
Terminal OS	<1.8.0

© Copyright 2026 B&R. All rights reserved.

Product	Affected versions
PVI	<6.9.0
ADI OPC UA Server	<3.0.0
OPC UA C/S TP	Not vulnerable

Vulnerability IDs

CVE-2025-15467, CVE-2025-11187

Summary

B&R is aware of public reports of a vulnerability in the product versions listed above.

An attacker who successfully exploited this vulnerability could cause the product to stop or insert and run arbitrary code.

Recommended immediate actions

Customers are advised to review if their systems parse untrusted PKCS#12 files or CMS/PKCS#7 content, as standard TLS usage (e.g., HTTPS handshakes) typically does not trigger these issues.

The problem is corrected in the following product versions:

Product	Patch version
mapp View	6.6.0
B&R Live Utils	3.0.2
B&R Linux 12	1.1.1
PPC80	1.8.2
PPT50	1.8.0
PPC50	1.8.0
PPT80	1.8.2
PFT51	1.8.2
PFT50	1.8.0
PPT30	1.8.0
Terminal OS	1.8.0
PVI	6.9.0 (pending)

© Copyright 2026 B&R. All rights reserved.

Product	Patch version
ADI OPC UA Server	3.0.0

B&R recommends that impacted customers apply the update at earliest convenience.

The process to install updates is described in the user manual. The step to identify the installed product version is described in the user manual.

Vulnerability severity and details

Vulnerabilities exist in the OpenSSL component included in the product versions listed above. Attackers could exploit these OpenSSL vulnerabilities by sending crafted PKCS#12 files or CMS/PKCS#7 messages with malformed parameters, potentially triggering stack buffer overflows or NULL pointer issues during parsing.

- CVE-2025-11187: Trick users/apps into importing malicious PKCS#12 (local file vector), may cause crashes or code execution.
- CVE-2025-15467: Remote delivery via CMS content (e.g., S/MIME), overflows stack pre-auth, could enable DoS or RCE.

TLS-only setups may avoid exposure, as standard TLS handshakes do not use the affected components.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS)[1] for both v3.1[2] and v4.0[3].

The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list[4].

CVE-2025-11187 Improper validation of PBMAC1 parameters in PKCS#12 MAC verification

PBMAC1 parameters in PKCS#12 files are missing validation which can trigger a stack-based buffer overflow, invalid pointer or NULL pointer dereference during MAC verification. Impact summary: The stack

[1] Common Vulnerability Scoring System (CVSS), Forum of Incident Response and Security Teams, Inc., https://www.first.org/cvss/.

[2] For the CVSS v3.1 scoring only the CVSS Base Score and the Temporal Score (if information is available) are considered in this advisory. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

[3] For the CVSS v4.0 scoring only the CVSS Base Metrics and the CVSS Supplemental Metrics (if information is available) are considered in this advisory. The CVSS Environmental and Threat Metrics, which can affect the vulnerability severity, are not provided in this advisory since they reflect the potential impact of a vulnerability within the end-user organizations' computing environment and over time depending on the vulnerability exploit maturity. Therefore, end-user organizations are recommended to analyze their situation and specify the Environmental and Threat Metrics.

[4] Common Weakness Enumeration (CWE), The MITRE Corporation, https://cwe.mitre.org/.

© Copyright 2026 B&R. All rights reserved.

buffer overflow or NULL pointer dereference may cause a crash leading to Denial of Service for an application that parses untrusted PKCS#12 files. The buffer overflow may also potentially enable code execution depending on platform mitigations. When verifying a PKCS#12 file that uses PBMAC1 for the MAC, the PBKDF2 salt and keylength parameters from the file are used without validation. If the value of keylength exceeds the size of the fixed stack buffer used for the derived key (64 bytes), the key derivation will overflow the buffer. The overflow length is attacker-controlled. Also, if the salt parameter is not an OCTET STRING type this can lead to invalid or NULL pointer dereference. Exploiting this issue requires a user or application to process a maliciously crafted PKCS#12 file. It is uncommon to accept untrusted PKCS#12 files in applications as they are usually used to store private keys which are trusted by definition. For this reason the issue was assessed as Moderate severity. The FIPS modules in 3.6, 3.5 and 3.4 are not affected by this issue, as PKCS#12 processing is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5 and 3.4 are vulnerable to this issue. OpenSSL 3.3, 3.0, 1.1.1 and 1.0.2 are not affected by this issue as they do not support PBMAC1 in PKCS#12.

CVSS

CVSS v3.1 Base Score:	6.1
CVSS v3.1 Temporal Score:	5.8
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:H/RL:O
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

CWE

CWE-476: NULL Pointer Dereference
CWE-787: Out-of-bounds Write

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2025-11187

CVE-2025-15467

Parsing CMS AuthEnvelopedData message with maliciously crafted AEAD parameters can trigger a stack buffer overflow. Impact summary: A stack buffer overflow may lead to a crash, causing Denial of Service, or potentially remote code execution. When parsing CMS AuthEnvelopedData structures that use AEAD ciphers such as AES-GCM, the IV (Initialization Vector) encoded in the ASN.1 parameters is copied into a fixed-size stack buffer without verifying that its length fits the destination. An attacker can supply a crafted CMS message with an oversized IV, causing a stack-based out-of-bounds write before any authentication or tag verification occurs. Applications and services that parse untrusted CMS or PKCS#7 content using AEAD ciphers (e.g., S/MIME AuthEnvelopedData with AES-GCM) are vulnerable. Because the overflow occurs prior to authentication, no valid key material is required to trigger it. While exploitability to remote code execution depends on platform and toolchain mitigations, the stack-based write primitive represents a severe risk. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the CMS implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3 and 3.0 are vulnerable to this issue. OpenSSL 1.1.1 and 1.0.2 are not affected by this issue.

CVSS

CVSS v3.1 Base Score:	9.8
CVSS v3.1 Temporal Score:	9.4
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O
CVSS v4.0 Score	N/A

© Copyright 2026 B&R. All rights reserved.

CVSS v4.0 Vector: N/A

CWE
CWE-787: Out-of-bounds Write

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2025-15467

Mitigating factors

For customers using OpenSSL solely for TLS (e.g., HTTPS or secure transport), exposure could be minimal since these vulnerabilities typically require processing specific certificate or signed data formats not involved in standard TLS handshakes.

Refer to section “General security recommendations” for further advise on how to keep your system secure.

Frequently asked questions

Could the vulnerabilities be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit these vulnerabilities. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

What does the update do?

The update removes the vulnerabilities by applying a fixed OpenSSL version.

When this security advisory was issued, had these vulnerabilities been publicly disclosed?

Yes, this vulnerability has been publicly disclosed.

When this security advisory was issued, had B&R received any reports that these vulnerabilities were being exploited?

No, B&R had not received any information indicating that these vulnerabilities were exploited when this security advisory was originally issued

General security recommendations

For any installation of software-related B&R products we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Isolate special purpose networks (e.g. for automation systems) and remote devices behind firewalls and separate them from any general-purpose network (e.g. office or home networks).
- Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.

© Copyright 2026 B&R. All rights reserved.

- Never connect programming software or computers containing programing software to any network other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.
- Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.
- Ensure all nodes are always up to date in terms of installed software, operating system, and firmware patches as well as anti-virus and firewall.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

More information on recommended practices can be found in the following documents:

Defense in Depth for B&R products

Support

For additional instructions and support please contact your local B&R service organization. For contact information, see https://www.br-automation.com/en/about-us/locations/.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.

Version history

Rev. Ind.	Page (p) Chapter (c)	Change description	Version. date
1.0	all	Initial version	09.11.2026

© Copyright 2026 B&R. All rights reserved.