DOCUMENT ID: SA26P010
VERSION: 1.0
DATE: 2026-06-11

CYBER SECURITY ADVISORY

Impact of Linux Kernel vulnerabilities on B&R products

CVE ID: CVE-2026-31431, CVE-2026-46300, CVE-2026-43284, CVE-2026-46333, CVE-2026-43494

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.

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 has thoroughly assessed its products for the identified vulnerabilities. The vulnerabilities can potentially be exploited in the products listed below:

- Linux for B&R <=12
- APROL < APROL-AutoYaST-DVD- V4.4-010.10.260602
- X20EDS410 all versions

For products not listed, no attack vector has been identified.

This may be due to one of the following reasons: the vulnerable component is not in use, the product design does not allow an attacker to perform the steps required to execute the attack, or the product already operates with root privileges by design as part of its intended use.

Important note: Some B&R products are designed to operate on a Linux-based host operating system. Independently of the vulnerabilities described in this advisory, customers are required to apply appropriate cyber hygiene measures to their host operating systems on an ongoing basis. This includes, but is not limited to, continuous vulnerability monitoring and the timely application of security patches.

Vulnerability IDs

CVE-2026-31431, CVE-2026-46300, CVE-2026-43284, CVE-2026-46333, CVE-2026-43494

Summary

B&R is aware of publicly reported vulnerabilities affecting the Linux kernel versions shipped with the products listed in this advisory. Successful local exploitation of these vulnerabilities could allow an attacker to escalate privileges on the affected system. Public proof-of-concept exploits are available for the vulnerabilities described herein. At the time of publication of this advisory, B&R had no evidence of active exploitation targeting B&R products.

Recommended immediate actions

For affected products, software updates should be installed upon availability.

Product	Patch version
Linux for B&R	pending
APROL	APROL-AutoYaST-DVD- V4.4-010.10.260602
X20EDS410	pending

Until remediated software versions are available, customers are required to conduct a risk assessment of their affected systems and to implement the mitigation measures and workarounds specified in this advisory.

Vulnerabilities severity and details

Several vulnerabilities exist in the Linux Kernel included in the product versions listed above. An attacker with local privileges on the system could exploit the vulnerabilities to elevate their privileges.

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].

[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/.

CVE-2026-31431

In the Linux kernel, the following vulnerability has been resolved: crypto: algif_aead - Revert to operating out-of-place This mostly reverts commit 72548b093ee3 except for the copying of the associated data. There is no benefit in operating in-place in algif_aead since the source and destination come from different mappings. Get rid of all the complexity added for in-place operation and just copy the AD directly.

CVSS

CVSS v3.1 Base Score: 7.8
CVSS v3.1 Temporal Score: 7.8
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RC:C

CVSS v4.0 Score N/A
CVSS v4.0 Vector: N/A

CWE

CWE-669: Incorrect Resource Transfer Between Spheres

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2026-31431

CVE-2026-43284

In the Linux kernel, the following vulnerability has been resolved: xfrm: esp: avoid in-place decrypt on shared skb frags MSG_SPLICE_PAGES can attach pages from a pipe directly to an skb. TCP marks such skbs with SKBFL_SHARED_FRAG after skb_splice_from_iter(), so later paths that may modify packet data can first make a private copy. The IPv4/IPv6 datagram append paths did not set this flag when splicing pages into UDP skbs. That leaves an ESP-in-UDP packet made from shared pipe pages looking like an ordinary uncloned nonlinear skb. ESP input then takes the no-COW fast path for uncloned skbs without a frag_list and decrypts in place over data that is not owned privately by the skb. Mark IPv4/IPv6 datagram splice frags with SKBFL_SHARED_FRAG, matching TCP. Also make ESP input fall back to skb_cow_data() when the flag is present, so ESP does not decrypt externally backed frags in place. Private nonlinear skb frags still use the existing fast path. This intentionally does not change ESP output. In esp_output_head(), the path that appends the ESP trailer to existing skb tailroom without calling skb_cow_data() is not reachable for nonlinear skbs: skb_tailroom() returns zero when skb->data_len is nonzero, while ESP tailen is positive. Thus ESP output will either use the separate destination-frag path or fall back to skb_cow_data().

CVSS

CVSS v3.1 Base Score: 7.8
CVSS v3.1 Temporal Score: 7.8
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

CVSS v4.0 Score N/A
CVSS v4.0 Vector: N/A

CWE

CWE-123: Write-what-where Condition

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2026-43284

CVE-2026-46333

In the Linux kernel, the following vulnerability has been resolved: ptrace: slightly saner 'get_dumpable()' logic The 'dumpability' of a task is fundamentally about the memory image of the task - the concept comes from whether it can core dump or not - and makes no sense when you don't have an associated mm. And almost all users do in fact use it only for the case where the task has a mm pointer. But we have one odd special case: ptrace_may_access() uses 'dumpable' to check various other things entirely independently of the MM (typically explicitly using flags like PTRACE_MODE_READ_FSCREDS). Including for threads that no longer have a VM (and maybe never did, like most kernel threads). It's not what this flag was designed for, but it is what it is. The ptrace code does check that the uid/gid matches, so you do have to be uid-0 to see kernel thread details, but this means that the traditional "drop capabilities" model doesn't make any difference for this all. Make it all make a *bit* more sense by saying that if you don't have a MM pointer, we'll use a cached "last dumpability" flag if the thread ever had a MM (it will be zero for kernel threads since it is never set), and require a proper CAP_SYS_PTRACE capability to override.

CVSS

CVSS v3.1 Base Score: 7.1
CVSS v3.1 Temporal Score: N/A
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

CVSS v4.0 Score N/A
CVSS v4.0 Vector: N/A

CWE

CWE-269: Improper Privilege Management

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/cve-2026-46333

CVE-2026-46300

In the Linux kernel, the following vulnerability has been resolved: net: skbuff: preserve shared-frag marker during coalescing skb_try_coalesce() can attach paged frags from @from to @to. If @from has SKBFL_SHARED_FRAG set, the resulting @to skb can contain the same externally-owned or page-cache-backed frags, but the shared-frag marker is currently lost. That breaks the invariant relied on by later in-place writers. In particular, ESP input checks skb_has_shared_frag() before deciding whether an uncloned nonlinear skb can skip skb_cow_data(). If TCP receive coalescing has moved shared frags into an unmarked skb, ESP can see skb_has_shared_frag() as false and decrypt in place over page-cache backed frags. Propagate SKBFL_SHARED_FRAG when skb_try_coalesce() transfers paged frags. The tailroom copy path does not need the marker because it copies bytes into @to's linear data rather than transferring frag descriptors..

CVSS

CVSS v3.1 Base Score: 7.8
CVSS v3.1 Temporal Score: N/A
CVSS v3.1 Vector CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Score N/A
CVSS v4.0 Vector: N/A

CWE
CWE-787: Out-of-bounds Write

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2026-46300

CVE-2026-43494

In the Linux kernel, the following vulnerability has been resolved: net/rds: reset op_nents when zerocopy page pin fails When iov_iter_get_pages2() fails in rds_message_zcopy_from_user(), the pinned pages are released with put_page(), and rm->data.op_mmp_znotifier is cleared. But we fail to properly clear rm->data.op_nents. Later when rds_message_purge() is called from rds_sendmsg() the cleanup loop iterates over the incorrectly non zero number of op_nents and frees them again. Fix this by properly resetting op_nents when it should be in rds_message_zcopy_from_user().

CVSS

CVSS v3.1 Base Score: 7.8
CVSS v3.1 Temporal Score: N/A
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Score N/A
CVSS v4.0 Vector: N/A

CWE
N/A

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2026-43494

Mitigating factors

Successful exploitation of the vulnerabilities described in this advisory requires local access to the affected system with low-privileged user credentials. Customers are strongly advised to enforce strict access control policies on all Linux-based systems, ensuring that interactive access is exclusively granted to authorized and trusted personnel. This includes reviewing and hardening user account permissions and disabling unused accounts.

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

Workarounds

Security researchers have identified and validated the following workarounds to reduce exposure to the vulnerabilities described in this advisory. These measures do not remediate the underlying vulnerabilities but effectively block known attack vectors until patched software versions are deployed.

Important: Customers are advised to thoroughly test their systems after applying any of the listed workarounds. B&R has no visibility into customer-specific applications running on the underlying Linux

system. It is the customer's responsibility to assess whether the applied workarounds interfere with existing application workloads prior to deployment in production environments.

CVE-2026-31431 – Copy Fail

For Debian-based systems within an active support lifecycle, kernel patches addressing CVE-2026-31431 are already available via the official package repositories. Customers are strongly encouraged to apply these updates immediately by executing the following command:

sudo apt update && sudo apt upgrade

A system reboot is required after the upgrade for the updated kernel to take effect.

Temporary Mitigation: If an immediate system update is not feasible, the affected kernel module (algif_aead) can be disabled persistently. Security researchers have confirmed this measure effectively prevents exploitation of CVE-2026-31431.

Execute the following commands as root:

echo "install algif_aead /bin/false" > /etc/modprobe.d/disable-algif.conf

rmmod algif_aead 2>/dev/null || true

Impact assessment: Disabling the algif_aead module removes the AEAD socket interface from the kernel crypto API. This does not affect dm-crypt/LUKS, kTLS, IPsec/XFRM, OpenSSL, GnuTLS, NSS, or SSH. Applications explicitly configured to use the afalg engine or that directly bind aead, skcipher, or hash sockets via AF_ALG may be affected. To assess exposure prior to applying this workaround, run:

lsof | grep AF_ALG

CVE-2026-43284 – Dirty Frag

Until a remediated software version is released, the original vulnerability researcher recommends disabling the affected kernel modules by executing the following command as root:

sh -c "printf 'install esp4 /bin/false\ninstall esp6 /bin/false\ninstall rxrpc /bin/false\n' > /etc/modprobe.d/dirtyfrag.conf; rmmod esp4 esp6 rxrpc 2>/dev/null; true"

Impact assessment: Unloading the esp4, esp6, and rxrpc modules disables IPsec ESP transport for both IPv4 and IPv6 as well as the RXRPC kernel transport protocol. Customers relying on kernel-level IPsec ESP (e.g. XFRM-based VPN tunnels) or RXRPC-dependent services should evaluate the operational impact before applying this workaround.

CVE-2026-46300 – Fragnesia

CVE-2026-46300 is a high-severity local privilege escalation vulnerability in the Linux kernel's socket buffer handling (skb_try_coalesce()) within the XFRM/ESP-in-TCP subsystem. An unprivileged local attacker can achieve arbitrary byte writes into the kernel page cache, leading to reliable local root privilege escalation.

Temporary Mitigation: If the Dirty Frag workaround (CVE-2026-43284) has already been applied, no additional action is required—both vulnerabilities share the same attack surface (esp4/esp6 modules).

If no prior mitigation exists, execute the following commands as root:

sh -c "printf 'install esp4 /bin/false\ninstall esp6 /bin/false\ninstall rxrpc /bin/false\n' > /etc/modprobe.d/fragnesia.conf"

rmmod esp4 esp6 rxrpc 2>/dev/null || true

After applying the blocklist, clear the page cache to remove any potentially corrupted cached binaries:

echo 3 > /proc/sys/vm/drop_caches

Impact assessment: This workaround is identical to the Dirty Frag mitigation. Unloading esp4 and esp6 disables IPsec ESP transport for IPv4 and IPv6. Customers relying on kernel-level IPsec ESP (e.g., XFRM-based VPN tunnels) should evaluate operational impact. To verify whether IPsec is in use prior to applying this workaround, run:

ip xfrm state list

ip xfrm policy list

CVE-2026-46333 – ptrace Exit-Race (ssh-keysign-pwn)

CVE-2026-46333 is an information disclosure vulnerability in the Linux kernel's ptrace access-check path that enables local privilege escalation. The flaw allows an unprivileged local attacker to steal file descriptors from exiting SUID processes (e.g., ssh-keysign, chage) to read SSH host private keys or /etc/shadow.

Temporary Mitigation: Restrict ptrace capabilities using the Yama Linux Security Module. Execute as root:

echo "kernel.yama.ptrace_scope=2" > /etc/sysctl.d/99-ptrace-restrict.conf

sysctl --system

Defense-in-depth option: Remove the SUID bit from the known target binaries:

chmod u-s /usr/libexec/openssh/ssh-keysign 2>/dev/null

chmod u-s /usr/bin/chage

Impact assessment: Setting ptrace_scope=2 restricts ptrace attachment to processes with CAP_SYS_PTRACE. Unprivileged users will no longer be able to use debugging tools (gdb -p, strace -p, perf trace --pid) on their own processes. For most production servers, this is acceptable. Removing the SUID bit from ssh-keysign breaks host-based SSH authentication; removing it from chage prevents non-root users from querying their own password aging information.

CVE-2026-43494 – PinTheft (RDS Zero-Copy Double Free)

CVE-2026-43494 is a reference-counting bug in the Linux kernel's Reliable Datagram Sockets (RDS) subsystem. A failed zero-copy page-pin operation leaves stale accounting state, triggering a double free that can be exploited for local privilege escalation to root.

Temporary Mitigation: Disable the RDS kernel modules by executing the following commands as root:

echo “install rds /bin/false” > /etc/modprobe.d/disable-rds.conf

echo “install rds_tcp /bin/false” >> /etc/modprobe.d/disable-rds.conf

modprobe -r rds_tcp rds 2>/dev/null || true

Optional additional hardening: If io_uring is not required by any workload, it can be disabled to further reduce the attack surface:

echo "kernel.io_uring_disabled=2" >> /etc/sysctl.conf

sysctl -p

Impact assessment: Disabling the rds and rds_tcp modules removes Reliable Datagram Sockets functionality. This affects clustered databases, Oracle RAC deployments, or specialized network workloads that depend on RDS for inter-node communication. To assess whether RDS is in use prior to applying this workaround, run:

lsmod | grep -E '^rds'

ss -x | grep rds

If no output is returned, the modules are not currently in use.

Post-Mitigation Note

After applying any patched kernel version that addresses these CVEs, remove the corresponding workaround configuration files and restore normal system operation. Validate IPsec, ptrace-dependent, and RDS workloads after reverting mitigations.

Frequently asked questions

What causes the vulnerabilities?

The vulnerabilities are caused by a vulnerable Linux Kernel component

What might an attacker use the vulnerability to do?

An authenticated attacker with low privileges may elevate privileges to root.

Could the vulnerabilities be exploited remotely?

Yes, an attacker with privileges to login in a vulnerable 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.

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

B&R is aware of reports indicating that these vulnerabilities had been exploited at the time this security advisory was originally issued; however, no exploitation has been observed in B&R products.

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.
- 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	11.06.2025

Rev. Ind.	Page (p) Chapter (c)	Change description	Version. date