Westermo-26-06:
Statement on recent Linux Kernel Privilege Escalation Vulnerabilities (Copy Fail, Dirty Frag, Fragnesia, Dirty Clone, PinTheft, ssh-keysign-pwn)

Severity: **LOW** Publication date: **2026-07-01**

Description

During the past months more than a handful of Linux Kernel high severity local privilege-escalation vulnerabilities have surfaced. The issues have typically been related to cryptographic functionality of the Linux Kernel, which under certain circumstances allow a local user to modify the kernel in-memory cache. Successful exploitation may allow escalation of privileges to root.

Copy Fail (CVE-2026-31431)

Copy Fail is a Linux Kernel local privilege-escalation vulnerability. The issue is caused by a logic flaw in the Linux kernel cryptographic AEAD API via module algif_aead, which under certain conditions allows a local user to modify the in-memory cached copy of a privileged executable.

Dirty Frag (CVE-2026-43284 & CVE-2026-43500)

Dirty Frag, sometimes called Copy Fail 2, includes two vulnerabilities in the Linux Kernel subsystems ESP/XFRM (CVE-2026-43284) and RxRPC (CVE-2026-43500). Unsafe in-place cryptographic processing may allow a low-privileged user to exploit the page-cache contents of sensitive files to gain root privileges.

Fragnesia (CVE-2026-46300)

Fragnesia is another vulnerability in the ESP/XFRM subsystem similarly to Dirty Frag. The public exploit abuses a bug in XFRM ESP-in-TCP to gain arbitrary writes of sensitive read-only files in the kernel page cache.

Dirty Clone (CVE-2026-43503)

Dirty Clone can allow a low-privileged local user to gain root access by modifying the Linux page-cache contents of sensitive files, similar to Dirty Frag and Fragnesia. Exploitation requires CAP_NET_ADMIN, which may be obtained through namespaces created with the *unshare* command. Although capabilities are namespaced, the page cache is shared at the host level.

PinTheft (CVE-2026-43494)

PinTheft exploits a flaw in the net/RDS module of the Linux kernel, where a counter used for memory management is not correctly reset, resulting in a double-free vulnerability. A local attacker could exploit this to potentially execute unauthorized code.

ssh-keysign-pwn (CVE-2026-46333)

ssh-keysign-pwn exploits a flaw in elevated processes where there is a brief window to intercept file access before it fully terminates, e.g. via tool ssh-keysign or chage. Successful exploitation may lead to the disclosure of sensitive local files such as /etc/shadow or SSH private keys.

Affected products and versions

Westermo has identified that these vulnerabilities affect firmware in a subset of products:

Vulnerability	Affected	Not affected
Copy Fail (CVE-2026-31431)	Ibex OS, WeRT OS, egOS (<1.10.1), WAWRT	WeOS 5, WeOS 4, egOS (>=1.10.1)
Dirty Frag (CVE-2026-43284)	WeOS 5, WeOS 4	
Dirty Frag (CVE-2026-43500)		WeOS 5, WeOS 4
Fragnesia (CVE-2026-46300)	WeOS 5, WeOS 4	
Dirty Clone (CVE-2026-43503)		WeOS 5, WeOS 4
PinTheft (CVE-2026-43494)		WeOS 5, WeOS 4
ssh-keysign-pwn (CVE-2026-46333)	WeOS 5, WeOS 4	

Impact

Based on current analysis, no viable attack vector has been identified within the intended operating environment for any of the affected products. Exploitation requires shell access as a non-root user, and shell access in Westermo products is typically limited to administrator accounts.

The vulnerabilities do not provide access to resources or functionality beyond those already available to a highly privileged user with an administrator role. As such, the practical impact on affected systems is considered limited.

This assessment may be attributed to one or more of the following factors:

- The vulnerable component is not used in the affected product configuration.
- The product design prevents an attacker from performing the steps required to exploit the vulnerability.
- The product operates with elevated privileges by design as part of its intended functionality.

Severity

CVE	Westermo CVSS	CVE.org CVSS
CVE-2026-31431 (Copy Fail)	7.0	7.8
CVE-2026-43284 (Dirty Frag)	7.0	8.8
CVE-2026-43500 (Dirty Frag)	7.0	7.8
CVE-2026-46300 (Fragnesia)	7.0	7.8
CVE-2026-43503 (Dirty Clone)	7.0	8.8
CVE-2026-43494 (PinTheft)	7.0	7.8
CVE-2026-46333 (ssh-keysign-pwn)	7.0	7.1

Mitigation

Updates

Westermo recommends upgrading to the latest firmware version available for each Westermo product. The vulnerabilities have been removed with the following releases:

- egOS 1.10.1

If an update is not available or not required based on the impact assessment, no immediate action is necessary.

Workarounds

If an upgrade is not possible, the following actions can be performed to mitigate the vulnerabilities:

- Monitor for updates related to this vulnerability.
- Apply available software updates when released.
- Follow general cybersecurity best practices, such as restricting access to management interfaces and limiting administrative access to trusted users.

Recommendations
After performing any of the mitigations, the following steps are recommended:

- Remove unused accounts.
- Restrict user accounts to trusted users only.
- Limit Administrator account access to a small number of trusted users.
- Change the login credentials on previously vulnerable devices.
- Follow password best practices.
- Minimize exposure of the management interface.
- Limit physical access to the device console port.

Important note

Some Westermo products operate on or in conjunction with a Linux-based host operating system. Independently of the vulnerability described in this advisory, customers are responsible for applying appropriate cyber hygiene measures to their systems. This includes, but is not limited to, continuous vulnerability monitoring and the timely application of relevant security patches where applicable.

Westermo will continue to monitor the situation and update this advisory if new information regarding exploitability or impact becomes available.

Contact

Westermo strongly encourage anyone who is experiencing a product security issue to contact the Westermo PSIRT. Details are available under Report a vulnerability ▷ Westermo.

References

- Westermo Products:
  https://www.westermo.com/products/product-lines-and-brands
- Westermo Operating System - WeOS:
  https://www.westermo.com/solutions/weos
- WeOS 5 - User Guide:
  https://docs.westermo.com/weos/weos-5/
- CVE-2026-31431 (Copy Fail)
  https://www.cve.org/CVERecord?id=CVE-2026-31431
- CVE-2026-43284 (Dirty Frag)
  https://www.cve.org/CVERecord?id=CVE-2026-43284
- CVE-2026-43500 (Dirty Frag)
  https://www.cve.org/CVERecord?id=CVE-2026-43500
- CVE-2026-46300 (Fragnesia)
  https://www.cve.org/CVERecord?id=CVE-2026-46300
- CVE-2026-43503 (Dirty Clone)
  https://www.cve.org/CVERecord?id=CVE-2026-43503

- CVE-2026-43494 (PinTheft)
  https://www.cve.org/CVERecord?id=CVE-2026-43494
- CVE-2026-46333 (ssh-keysign-pwn)
  https://www.cve.org/CVERecord?id=CVE-2026-46333

Revision History

- 2026-07-01: Initial release