corero [NETWORK SECURITY]

Corero Network Security

Advisory of Corero Impact from CVE-2026-31431 Linux Kernel Vulnerability

Advisory ID: 05012026-2
Published: 6 May 2026
CVEs: CVE-2026-31431 – Linux Kernel Vulnerability

Summary

The recently disclosed vulnerability (CVE-2026-31431) affects the Linux kernel. If exploited, it allows an unprivileged user to gain root access. The CVE was made public on 22nd April 2026.

Corero solutions run the affected Rocky Linux version, but its hardened configuration blocks unprivileged shell access, so the vulnerability cannot be exploited.

Customers should continue to follow recommended best practice to restrict access to trusted sources only.

Impact Statement

The following Corero products **CANNOT BE EXPLOITED** by CVE-2026-31431:

- SmartWall Service Portal (SSP) – all versions since 3.0.0
- SmartWall SecureWatch Analytics (SWA) – all versions
- SmartWall ONE Central Management Server (CMS) - all versions
- SmartWall ONE Network Threat Defense (NTD) hardware appliances and software virtual machines - all versions
- SmartWall Threat Defense Director (TDD) - all versions

Corero will also include precautionary patches in its forthcoming release scheduled within June/July 2026.

Recommended Actions

Corero components should always be secured against this or other vulnerabilities by limiting access only to known / trusted IP addresses, using the pCLI *ip-filter* command. This command allows access only from the listed IP addresses or CIDRs, and blocks access from any unlisted IP address. This will block any attempt to exploit the vulnerability.

For example:

```
cms>setup ip-filter

  Would you like to enable IP filtering? <Y,[N]>: y

  Always allow ICMP? <[Y],N>:

  Please enter permitted IP list:

  ….
```

Note:

- Use the following SSH command to access a CMS or NTD pCLI: *ssh -p 2222 <adminUser>@<IPAddress>*
- When using ip-filter on the CMS, ensure you allow the IP address of all routers sending telemetry to that CMS.
- When using ip-filter on an NTD, ensure you allow the IP address of the CMS managing that NTD.
- The ip-filter configuration must be applied to each NTD.
- The ip-filter command takes IP addresses in CIDR format. A single IP must be expressed as a.b.c.d/32.

Corero also recommends following best practice whenever possible to secure your SmartWall ONE deployment, including connecting management interfaces to secure networks, isolated from the Internet.

Please contact your Corero support representative for more information.