Proxmox Virtual Environment - Security Advisories

ProxmoxSecurityAdvisory · Jan 1, 2024

Not open for further replies.

ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Aug 10, 2026 #61

Subject: PSA-2026-00037-1: SCTPhantom Local Privilege Escalation issue

Advisory date: 2026-08-10

Packages: proxmox-kernel-*

Details:

A use-after-free issue in the Linux kernels SCTP code allowed a unprivileged local attacker to obtain root privileges, and potentially escape from unprivileged containers.

Mitigations:

Preventing the `sctp` module from being loaded mitigates the issue.

Fixed in:
- proxmox-kernel-7.0.14-10-pve(-signed) (Trixie based products)
- proxmox-kernel-6.8.12-41-pve(-signed) (Bookworm based products)

References:
- CVE-2026-64564
- https://matrix.tencent.com/en/2026/08/06/sctphantom-CVE-2026-64564

ProxmoxSecurityAdvisory
Proxmox Staff Member

Aug 10, 2026 #62

Subject: PSA-2026-00038-1: TONTOU kernel memory leak via branch predictor re-poisoning

Advisory date: 2026-08-10

Staff member

Packages: proxmox-kernel-*

Details:

A new technique to leak kernel memory despite spectre v2 mitigations being in place to neutralize the branch predictor state was discovered. This technique uses interrupt injection to re-poison the branch predictor during the window between neutralization and return of execution.

This technique is only applicable on AMD and Intel CPUs.

Fixed in:
- proxmox-kernel-7.0.14-11-pve(-signed) (Trixie based products)
- proxmox-kernel-6.8.12-41-pve(-signed) (Bookworm based products)

References:
- CVE-2026-68480
- https://people.csail.mit.edu/mengjia/data/2026.USENIX.TONTOU.pdf (paper, PDF)



ProxmoxSecurityAdvisory
Proxmox Staff Member

Staff member

Aug 12, 2026 #63

Subject: PSA-2026-00039-1: missing parameter validation in remote migration

Advisory date: 2026-08-12

Packages: qemu-server

Details:

Missing parameter validation in Proxmox VE's remote migration code allowed an attacker with `Sys.Incoming` privileges to inject arbitrary values in parts of the QEMU command line on the migration target.

This issue was privately reported by Geoffrey McClinsey <geoffrey.mcclinsey@gmail.com>.

Fixed in:
- qemu-server >= 9.2.3 (PVE 9.x)
- qemu-server >= 8.4.9 (PVE 8.x)



ProxmoxSecurityAdvisory
Proxmox Staff Member

Aug 12, 2026 #64

Subject: PSA-2026-00040-1: incomplete privilege checks for unused volumes

Staff member

Advisory date: 2026-08-12

Packages: qemu-server, pve-container

Details:

Incomplete privilege checks when adding an unused volume to a guest allowed accessing volumes that were out of scope for the user/API token adding the volume.

This issue was reported privately by Geoffrey McClinsey <geoffrey.mcclinsey@gmail.com> for qemu-server, a related issue in pve-container was found while developing the fix.

Fixed in:
- qemu-server >= 9.2.2 (PVE 9.x)
- pve-container >= 6.1.13 (PVE 9.x)
- qemu-server >= 8.4.9 (PVE 8.x)
- pve-container >= 5.3.6 (PVE 8.x)

Aug 17, 2026 #65

Proxmox Staff Member

Staff member

Advisory date: 2026-08-17

Packages: pve-manager

Details:

Any authenticated user/API token could trigger a stop of running backups.

This issue was reported privately by Geoffrey McClinsey <geoffrey.mcclinsey@gmail.com>.

Fixed in:
- pve-manager >= 9.2.8 (PVE 9.x)
- pve-manager >= 8.4.20 (PVE 8.x)

Yesterday at 08:31 #66

ProxmoxSecurityAdvisory

Proxmox Staff Member

Staff member

Subject: PSA-2026-00043-1: Authentication bypass in EOL Proxmox VE 7 release

Advisory date: 2026-09-01

Packages: libpve-access-control

Affected: libpve-access-control >= 7.0-7 and < 8.0.4

Roughly corresponding to Proxmox VE 7.0 up to and including 7.4 (end of life since July 2024), and, for completeness, the initial Proxmox VE 8.0 (EOL), as the fix only shipped roughly one month after that release.

Package versions and the overall Proxmox VE version only correlate loosely, since dependency versions are only raised when needed. To determine whether an installation is affected, check the installed package version, not the overall Proxmox VE version:

```
dpkg-query -W -f '${Version}\n' libpve-access-control
```

Alternatively `pveversion -v` lists the versions of all installed Proxmox VE packages - look for the version of libpve-access-control.

Fixed in: libpve-access-control 8.0.4 (released 2023-07-20) and all later versions. No supported Proxmox VE release is affected.

Details:

The API login call (POST /api2/json/access/ticket) accepts a 'tfa-challenge' parameter. It carries the signed, half-authenticated TFA challenge ticket that a client receives when logging in as a user with two-factor authentication, and is used to complete the second factor.

In the affected versions, this parameter was not validated for users without configured second factors, while its presence also caused the verification of the submitted password to be skipped entirely. As a result, an attacker with access to the API could authenticate as any existing, enabled user without configured second factors (by default this includes root@pam), without knowing any credentials, by passing an arbitrary value in the 'tfa-challenge' parameter.

Exploitation requires access to the API port (8006), directly or through a reverse proxy. Restricting API access to trusted networks has always been our recommended setup.

Timeline:

The vulnerable code path was closed in July 2023, with libpve-access-control 8.0.4, as a side effect of a rework of the TFA configuration handling for an unrelated issue. At that time, the authentication bypass was not known: the rework was not a security fix, and the issue had neither been found internally nor reported. It was therefore not recognized as a candidate for a backport to the PVE 7 branch.

We learned of the issue now, through many independent reports within the last two days, which also report exploitation in the wild. Given the severity of the issue we are publishing this advisory for the affected end-of-life releases, including a stop-gap mitigation for installations that cannot upgrade right away.

The issue was independently reported by:
* Kamil Rakowski <kamil@kamilrak.com>
* Nathan Xavier Golez <nathan@nathangolez.com>
* Sagnik Sasmal <sagnik@sagnik.me>
* various LLMs

Mitigation:

Installations whose API is not reachable by potential attackers are not exposed. Further, users with any second factor configured for login are not affected.

For installations that cannot upgrade right away, the following patch adds a validation step to the affected code path: every 'tfa-challenge' value must then be a valid, signed TFA challenge ticket, which an attacker cannot forge. Normal password logins and two-factor logins keep working.

Bash:

```
sed -i.bck 's/^\t# This is the 2nd factor, use the password for the

grep -n 'verify_ticket($tfa_challenge, 0, $username)' /usr/share/per

systemctl reload-or-restart pvedaemon pveproxy
```

The grep command must print 3 (occurrences of the verify_ticket line in the file). If it prints anything else, the patch did not apply and the installation is still vulnerable. To undo the patch, restore the '.bck' backup file and restart both services again.

Upgrading to a supported Proxmox VE release is the only durable fix: the affected releases are end of life and have not received the security fixes shipped since then, both for the PVE stack itself and for components such as the Linux kernel, QEMU or LXC, among others.

References:

* CVE-2023-54391

Prev 1 2 3 4

Not open for further replies.

Share:

About

Quick Navigation

We value your privacy

We use essential cookies to make this site work, and optional cookies to enhance your experience.

See further information and configure your preferences

Accept all cookies

Reject optional cookies

The Proxmox team works very hard to make sure you are running the best software and getting stable updates and security enhancements, as well as quick enterprise support. Tens of thousands of happy customers have a Proxmox subscription. Get yours easily in our online shop.

Buy now!

Community platform by XenForo® © 2010-2026 XenForo Ltd.