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)

Sep 1, 2026 #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



ProxmoxSecurityAdvisory
Proxmox Staff Member

Staff member

Sep 10, 2026 #67

Subject: PSA-2026-00044-1: XSS in various UI components

Advisory date: 2026-09-10

Packages: pve-manager

Details:

Various dialogues in the web interface were susceptible to XSS:
- The VM `Hardware` panel, because of the `romfile` for PCI devices. This requires an attacker to have the `Mapping.Use` privilege for a PCI mapping.
- The VM `Cloud-Init` panel, because of the `searchdomain` field. This requires an attacker to have the `VM.Config.Cloudinit` or `VM.Config.Network` privilege for a VM.
- The node's `Certificates` panel, because of the `Subject Alternative Names` field. This requires an attacker to have the `Sys.Modify` privilege for a node.

The issues for the VM panels were privately reported by Geoffrey McClinsey <geoffrey.mcclinsey@gmail.com>.
The issues with the certificates component, were privately reported by Nguyen Van Thuy <nvthuy37@gmail.com> and Luong Huynh Minh Kien <lhminhkien1992@outlook.com>.

Fixed in:
- pve-manager >= 9.2.11 (PVE 9.x)
- proxmox-widget-toolkit >= 5.2.8 (PVE 9.x)
- pve-manager >= 8.4.21 (PVE 8.x)
- proxmox-widget-toolkit >= 4.3.18 (PVE 8.x)

Last edited: Sep 10, 2026



ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Sep 10, 2026 #68

Subject: PSA-2026-00046-1: Privilege escalation through malicious OCI container image

Advisory date: 2026-09-10

Packages: pve-container

Details:

The check for control characters in the configuration keys of OCI container images was too permissive, allowing a user with privileges to upload a malicious image to inject lines into the generated LXC configuration of containers created using this OCI image.

This could be used trigger execution of arbitrary commands as root on the host.

The issue was privately reported by Finn van der Knaap.

Fixed in:
- pve-container >= 6.1.14

ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Sep 21, 2026 #69

Subject: PSA-2026-00047-1: newline injection into firewall config files

Advisory date: 2026-09-21

Packages: pve-firewall, proxmox-firewall

Details:

Incomplete validation of API parameters allowed the injection of newlines or invalid lines into firewall configuration files.

The original issue was reported privately by Geoffrey McClinsey <geoffrey.mcclinsey@gmail.com>. Further related issues were found and fixed while developing the fix.

Fixed in:
- pve-firewall >= 6.0.6
- libpve-common-perl >= 9.2.2

ProxmoxSecurityAdvi

Sep 21, 2026 #70

Subject: PSA-2026-00050-1: password change via incomplete username validation

We value your privacy

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

Accept all cookies

See further information and configure your preferences

Reject optional cookies

An attacker with sufficient privileges to create new PAM user entries (`Realm.AllocateUser` on `/access/realm/pam`) could change the PAM password of arbitrary existing users, while disabling them in Proxmox VE's user.cfg at the same time.

An attacker with sufficient privileges to create new user entries in a realm (`Realm.AllocateUser` on `/access/realm/{realm}`) could change the password of arbitrary existing users, while disabling them in Proxmox VE's user.cfg at the same time, provided the realm allows setting of passwords via the corresponding authentication plugin.

Both variants circumvent restrictions on password changes which normally apply:
- password changes in the PAM realm are only available to `root@pam`

- password changes in general require `User.Modify` on the modified user's groups, if the modified user is a member of any groups

This issue was discovered internally.

Fixed in:
- libpve-access-control >= 9.1.2



ProxmoxSecurityAdvisory
Proxmox Staff Member

Staff member

Sep 24, 2026 #71

Subject: PSA-2026-00051-1: integrity bypass of encrypted backups on an untrusted PBS instance

Advisory date: 2026-09-24

Packages: proxmox-backup-client, proxmox-backup-file-restore, libproxmox-backup-qemu0

Details:

When a PBS client is configured with an encryption/signing key, it silently accepted a backup manifest that carried no signature. An attacker with write access to the PBS server could replace a signed manifest with an unsigned one, defeating the integrity guarantee that client-side encryption and signatures are meant to provide when interacting with an untrusted server/storage.

This is an integrity-only issue: the attacker never learns the encryption key or original plaintext, so confidentiality of the encrypted backup itself is not affected.

Whenever a client is configured with an encryption/signing key, it will now only trust signed manifests, unless explicitly overridden using a newly introduced flag.

Note: The Proxmox VE storage integration currently does not provide an override to allow accessing unsigned backups if a PBS storage is configured with an encryption key. To access plain text backups made before setting up encryption, or synced without encryption from another source on the PBS side, move or sync such backups to a different namespace and configure that namespace as additional PBS storage.

This issue was reported privately by Shaun Mirani, and later independently by Project Loupe.

Fixed in:
- proxmox-backup-client(-static), proxmox-backup-file-restore >= 4.2.6-1
- libproxmox-backup-qemu0 >= 2.0.3

ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Oct 1, 2026 #72

Subject: PSA-2026-00052-1: Command injection via import of malicious OVA file

Advisory date: 2026-10-01

Packages: libpve-storage-perl, qemu-server

Details:

Insufficient restrictions of OVA member file names allowed an attacker with sufficient privileges to upload and import OVA files to inject arbitrary arguments into a `tar` invocation executed as root.

This issue was found and reported privately by Project Loupe.

Fixed in:
- libpve-storage-perl >= 9.1.11

ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Oct 1, 2026 #73

Subject: PSA-2026-00053-1: PBS backup access includes `host/NNN` groups

Advisory date: 2026-10-01

Packages: libpve-storage-perl

Details:

If a configured PBS storage contained backup groups with type `host`, but numerical backup IDs, such snapshots were treated like guest backups despite their mismatching type.

An attacker with `VM.Backup` privilege on the "guest ID" and `Datastore.AllocateSpace` on the storage could trigger a file restore task or other actions on such a host backup.

This issue was reported privately by Project Loupe.

Fixed in:
- libpve-storage-perl >= 9.1.11

ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Oct 7, 2026 #74

Subject: PSA-2026-00059-1: pxar/container restore target rootfs escape

Advisory date: 2026-10-07

Packages: pve-container, proxmox-backup-client, rust-pxar

Details:

An attacker with direct access to a PBS datastore configured as storage on a Proxmox VE host can construct and upload a malicious pxar archive with two root entries.

When such a backup archive was restored by pve-container, the archive contents were written outside of the target rootfs mountpoint. If a container is restored as privileged container, the extraction runs as root.

proxmox-backup-client will now refuse to follow symlinks during extraction of directories or hardlinks.

This issue was reported privately by Project Loupe.

Fixed in:
- proxmox-backup-client >= 4.2.7-1

ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Oct 12, 2026 #75

Subject: PSA-2026-00066-1: ESXi importer: path traversal in vmx parser

Advisory date: 2026-10-12

Packages: libpve-storage-perl

Details:

Incomplete path validation in the ESXi importer allowed an attacker with access to a configured ESXi instance with privileges to trigger imports to leak arbitrary file contents of paths ending in `.vmx`.

This issue was reported privately by Ibrahim Aljaafreh from Cystack RedTeam.

Fixed in:
- libpve-storage-perl >= 9.1.12

ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Oct 15, 2026 #76

Subject: PSA-2026-00067-1: VMA extraction path escape

Advisory date: 2026-10-15

Packages: pve-qemu-kvm

Details:

An attacker restoring a crafted VMA file could trigger overwrites of arbitrary host paths.

Note: writing "raw" VMA files is not possible via the PVE API or backup feature, but requires direct access to the filesystem where backup archives are stored.

This issue was found internally.

Fixed in:
- pve-qemu-kvm >= 11.1.1-2 (Qemu 11.1+)
- pve-qemu-kvm >= 11.0.3-4 (Qemu 11.0)

ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Oct 16, 2026 #77

Subject: PSA-2026-00068-1: "PwnEscape" Guest-to-Host KVM Escape

Advisory date: 2026-10-16

Packages: proxmox-kernel

Details:

Incomplete validation of network packet checksum metadata when completing the checksum calculation allowed an attacker to read host memory and write host kernel memory via the virtio network stack, allowing an escape from inside a KVM guest.

Fixed in:
- proxmox-kernel-7.0.14-24-pve(-signed)

References:
- CVE-2026-99999
- https://pwn.ai/blog/pwnescape

ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Oct 19, 2026 #78

Subject: PSA-2026-00069-1: Missing redaction of cloudinit cipassword in snapshot config endpoint

Advisory date: 2026-10-19

Packages: qemu-server

Details:

The VM-related endpoint `/snapshot/{snap}/config` for querying the configuration of a snapshot, did not mask the `cipassword` field in the result. When the snapshot configuration or current configuration is queried via `/config`, the `cipassword` field is already masked.

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

Fixed in:
- qemu-server >= 9.2.11

References: Advisory PSA-2026-00017-1 was about a similar issue for the `cloudinit/dump` endpoint.

ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Oct 19, 2026 #79

Subject: PSA-2026-00070-1: Missing storage access check when configuring custom cloud-init snippets for a VM

Advisory date: 2026-10-19

Packages: qemu-server

Details:

A user with the `VM.Config.Cloudinit` privilege could reference volumes from any storage via the `cicustom` property. If the user also has permissions to start the VM and guest access, they can thus read the contents of snippet volumes from any storage. An existing check blocks VM startup when the volume type for a volume referenced by `cicustom` is not `snippets`. Note that guest hookscripts and backup hookscripts are also snippet volumes.

This issue was privately reported by Geoffrey McClinsey <geoffrey.mcclinsey@gmail.com>, and independently by Ibrahim AlJaafreh <ibrahim0aljaafreh@gmail.com>, Project Loupe and Yuliang Xiao.

Fixed in:
- qemu-server >= 9.2.11



ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Oct 19, 2026 #80

Subject: PSA-2026-00071-1: Incomplete privilege checks for cloudinit config changes

Advisory date: 2026-10-19

Packages: qemu-server

Details:

An attacker with `VM.Config.Network` privileges on a VM could change cloud-init settings relating to authentication within the VM, which would otherwise require the `VM.Config.Cloudinit` privilege.

Note: normally, these settings only have an effect inside the VM on first boot, or after changing the instance-id.

This issue was privately reported by Project Loupe.

Fixed in:
- qemu-server >= 9.2.11

Prev 1 2 3 4 5 Next

Not open for further replies.

Share:

Forums > Proxmox > Security Advisories

About

The Proxmox community has been around for many years and offers help and support for Proxmox VE, Proxmox Backup Server, and Proxmox Mail Gateway.

Quick Navigation

Home

Get Subscription

We think our community is one of the best thanks to people like you!

Wiki

Downloads

Proxmox Customer Portal

About

Get your subscription!

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!

Cookies Proxmox Support Forum - Light Mode

Contact us Terms and rules Privacy policy Help Home

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