Proxmox Mail Gateway - Security Advisories

ProxmoxSecurityAdvisory · Jan 1, 2024

Not open for further replies.

ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Jan 1, 2024 #1

This is the list of security advisories since 2024-01-01 for the Proxmox Mail Gateway.

For details about scope, coverage and timeline see the General FAQ about Proxmox Security Announcements.

ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Mar 28, 2024 #2

Subject: PSA-2024-00005-1: SMTP Smuggling

Publication date: 2024-03-28

Packages: pmg-api, postfix

Details: Postfix was affected by an email spoofing attack that involves a composition of email services with specific differences in the way they handle line endings other than <CR><LF>. See references below for timeline, mitigations and details.

Fixed:
- pmg-api >= 8.0.10 (Proxmox Mail Gateway 8.x)
- pmg-api >= 7.3-11 (Proxmox Mail Gateway 7.x)

References:
- CVE-2023-51764
- https://www.postfix.org/smtp-smuggling.html
- https://forum.proxmox.com/threads/smtp-smuggling-mitigation.138576/

Jun 28, 2024 #3

ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Subject: PSA-2024-00007-1: Shim bootloader remote code execution via http response

Advisory date: 2024-06-28

Packages: shim-unsigned, shim-signed

Details: A remote code execution vulnerability was found in the secure boot Shim bootloader. The Shim boot support trusts attacker-controlled values when parsing an HTTP response. This flaw allows an attacker to craft a specific malicious HTTP request, leading to a completely controlled out-of-bounds write primitive and complete system compromise. This flaw is only exploitable during the early boot phase, an attacker needs to perform a Man-in-the-Middle or compromise the boot server to be able to exploit this vulnerability successfully.

Fixed: shim-unsigned >= 15.8, shim-signed >= 1.40+pmx1+15.8 (Proxmox VE 8.x, Proxmox Backup Server 3.x, Proxmox Mail Gateway 8.x)

Bullseye-based Proxmox products do not ship a custom version of shim, refer to Debian's security tracker if manual secure boot is in use.

References: CVE-2023-40547, shim 15.8 additionally fixes CVE-2023-40546 and CVE-2023-40548 to CVE-2023-40551

Sep 23, 2024 #4

ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Subject: PSA-2024-00009-1: Proxmox VE/Mail Gateway API: post-authentication privileged file read vulnerabilities

Advisory date: 2024-09-23

Packages:
- Proxmox Virtual Environment: pve-manager, libpve-storage-perl, libpve-http-server-perl, qemu-server
- Proxmox Mail Gateway: pmg-api, libpve-http-server-perl

Details:
Insufficient safeguards against malicious API response values allowed authenticated attackers with 'Sys.Audit' or 'VM.Monitor' privileges to download arbitrary host files via the API.

Two instances of this issue were discovered and reported by the Security Labs team at Snyk.
The issue was introduced in libpve-http-server-perl in version 3.2-1 (Proxmox VE/Proxmox Mail Gateway 6) with commit 6d832db ("allow 'download' to be passed from API handler").

Timeline:
2024-09-04: initial report by Snyk

2024-09-04: initial analysis and acknowledgment by Proxmox Security Team
2024-09-06: first iteration of patches submitted for internal review and testing
2024-09-12: second iteration of patches submitted for internal review and testing
2024-09-13: patches and tentative roll-out timeline submitted for feedback to Snyk
2024-09-13: status quo of affected packages was bumped and rolled out to reduce regression potential
2024-09-19: third iteration of patches with minor usability and backward compatibility improvements submitted for internal review and testing
2024-09-20: Due to impact, an exception was granted to provide fixes for the EOL Proxmox VE 7 and Proxmox Mail Gateway 7 releases and a backport of the patches got submitted for internal review and testing
2024-09-23: coordinated release of fixed packages to the Proxmox VE and Proxmox Mail Gateway repositories of the 7 and 8 release series.

Fixed:
- Proxmox VE 8:
pve-manager >= 8.2.7, libpve-storage-perl >= 8.2.5, libpve-http-server-perl >= 5.1.1,
(libpve-common-perl >= 8.2.3, only cosmetic changes to reduce misuse potential)

- Proxmox Mail Gateway 8:
pmg-api >= 8.1.4, libpve-http-server-perl >= 5.1.1, (libpve-common-perl >= 8.2.5)

- Proxmox Virtual Environment 7:
pve-manager >= 7.4-19, libpve-storage-perl >= 7.4-4, libpve-http-server-perl >= 4.3.0

- Proxmox Mail Gateway 7:
pmg-api >= 7.3-12, libpve-http-server-perl >= 4.3.0

References:
- CVE-2024-21545 (reserved)



ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Dec 12, 2024 #5

Subject: PSA-2024-00012-1: Proxmox Mail Gateway: unexpected handling of single-part attachments

Advisory date: 2024-12-12

Packages: pmg-api

Details:
The Remove Attachments and Attachment Quarantine actions in the rule system ignored the `Content-Disposition: attachment` header for the first MIME part of the mail, which is usually the part containing the mail-text. As e-mails with malicious content do use unexpected header combinations to confuse mail-filters, removing more parts, in case of doubt, is the proper behavior. Additionally, this behavior is

more in line with many mail user agents, which treat such mail parts as attachment.

The issue was responsibly reported by Philipp Hutterer <Hutterer@develop-group.de> with a sample mail that contained a single-part attachment, which was not removed.

Fixed:
- pmg-api version 8.1.5



ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Dec 18, 2024 #6

Subject: PSA-2024-00015-1: XSS in mail queue fields

Advisory date: 2024-12-18

Packages: pmg-gui

Details:
Missing encoding in the Proxmox Mail Gateway UI led to HTML code contained in fields of the mail queue view to be rendered by the browser.

This issue was reported by Niels Hendriks from Rootnet.

Fixed: pmg-gui >= 4.1.2



ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Mar 6, 2025 #7

Subject: PSA-2025-00005-1: Various SecureBoot bypasses, data integrity violations and sensitive data leaks in Grub

Advisory date: 2025-03-06

Packages: grub-pc-bin, grub-efi-amd64-bin, grub-efi-amd64-signed, grub-efi-amd64-unsigned

Details:

21 issues in Grub's codebase were found that could allow an attacker to bypass Secure Boot protections (if enabled), leak sensitive data from Grub's environment or configuration or violate other integrity protections within Grub.

Fixed:
- grub-pc-bin (>= 2.06-13+pmx5)
- grub-efi-amd64-bin (>= 2.06-13+pmx5)
- grub-efi-amd64-unsigned (>= 2.06-13+pmx5)
- grub-efi-amd64-signed (>= 1+2.06+13+pmx5)
- proxmox-secure-boot-policies (>= 0.0~git20240117.c443a5f-5)

- proxmox-secure-boot-policies-amd64-signed (>= 0.0~git20240117.c443a5f-5)

To fully prevent downgrade attacks after upgrading to fixed versions of the packages, see the instructions in our wiki:

https://pve.proxmox.com/wiki/Secure_Boot_Setup#Setting_a_Stricter_Revocation_Policy

References:
CVE-2024-45774: reader/jpeg: Heap OOB Write during JPEG parsing.
CVE-2024-45775: commands/extcmd: Missing check for failed allocation.
CVE-2024-45776: grub-core/gettext: Integer overflow leads to Heap OO Write and Read.
CVE-2024-45777: grub-core/gettext: Integer overflow leads to Heap OOB Write.
CVE-2024-45778: fs/bfs: Integer overflow in the BFS parser.
CVE-2024-45779: fs/bfs: Integer overflow leads to Heap OOB Read (Write?) in the BFS parser.
CVE-2024-45780: fs/tar: Integer Overflow causes Heap OOB Write.
CVE-2024-45781: fs/ufs: OOB write in the heap.
CVE-2024-45782: fs/hfs: strcpy() using the volume name (fs/hfs.c:382)
CVE-2024-45783: fs/hfs+: refcount can be decremented twice
CVE-2025-0622: command/gpg: Use-after-free due to hooks not being removed on module unload
CVE-2025-0624: net: Out-of-bounds write in grub_net_search_config_file()
CVE-2025-0677: UFS: Integer overflow may lead to heap based out-of-bounds write when handling symlinks
CVE-2025-0678: squash4: Integer overflow may lead to heap based out-of-bounds write when reading data
CVE-2025-0684: reiserfs: Integer overflow when handling symlinks may lead to heap based out-of-bounds write when reading data
CVE-2025-0685: jfs: Integer overflow when handling symlinks may lead to heap based out-of-bounds write when reading data
CVE-2025-0686: romfs: Integer overflow when handling symlinks may lead to heap based out-of-bounds write when reading data
CVE-2025-0689: udf: Heap based buffer overflow in grub_udf_read_block() may lead to arbitrary code execution
CVE-2025-0690: read: Integer overflow may lead to out-of-bounds write
CVE-2025-1118: commands/dump: The dump command is not in lockdown when secure boot is enabled
CVE-2025-1125: fs/hfs: Integer overflow may lead to heap based out-of-bounds write



ProxmoxSecurityAdvisory
Proxmox Staff Member

Staff member

Jul 10, 2025 #8

Subject: PSA-2025-00012-1: Incomplete exclusion of the NTFS module in Grub2 with Secure Boot

Advisory date: 2025-07-10

Packages: grub-efi-amd64-signed 1+2.06+13+pmx6

Details: The NTFS fixes for the issues described in PSA-2025-00005-1 were reverted

setups that enable Secure Boot. To fix this, exclude the NTFS module from being part of the monolithic GRUB EFI binary.

Fixed: grub-efi-amd64-signed 1+2.06+13+pmx7

References: PSA-2025-00005-1



ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Sep 4, 2025 #9

Subject: PSA-2025-00015-1: stored XSS in config values

Advisory date: 2025-09-04

Packages: pmg-gui

Details: The HTTP proxy setting dialogue in the web interface was susceptible to XSS. Editing this setting is only available to users with `admin` level access.

A related issue in the Proxmox VE code base was discovered and reported by Javidan Khankishiyev <Khankishiyev.j@gmail.com>.

Fixed: pmg-gui >= 4.2.1



ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Sep 17, 2025 #10

Subject: PSA-2025-00016-1: Spectre branch target injection from VM guests ("VMScape")

Advisory date: 2025-09-17

Packages: proxmox-kernel-6.8, proxmox-kernel-6.14

Details: Incomplete branch predictor isolation mechanisms allow exploitation of branch prediction across hypervisor/guest context switches, potentially leaking secrets from the host userspace or other guests by an attacker with control over a VM.

Fixed:

For Debian Trixie based releases, like Proxmox VE 9, Proxmox Backup Server 4 or Proxmox Datacenter Manager Beta:
- Package `proxmox-kernel-6.14.11-2-pve-signed` in version `6.14.11-2`

For Debian Bookworm based releases, like Proxmox VE 8, Proxmox Backup Server 3 or Proxmox Mail Gateway 8:
- Package `proxmox-kernel-6.14.8-3-bpo12-pve-signed` in version `6.14.8-3~bpo12+1`
- Package `proxmox-kernel-6.8.12-15-pve-signed` in version `6.8.12-15`

References:
- CVE-2025-40300
- https://comsec.ethz.ch/research/mic...ch-predictor-isolation-in-cloud-environments/



ProxmoxSecurityAdvisory
Proxmox Staff Member

Staff member

Jan 13, 2026 #11

Subject: PSA-2026-00001-1: Authenticated Remote Code Execution via shell injection

Advisory date: 2026-01-13

Packages: pmg-api

Details: Missing separation between options and package name arguments in an `apt-get` invocation exposed over the API allowed an authenticated attacker with Sys.Audit privileges to inject arbitrary options into the resulting apt-get command line. Such an attacker could inject options that trigger arbitrary code execution as `www-data`.

The vulnerable API endpoint is only available to authenticated admin users, quarantine-level access does not allow exploiting it.

This issue was found and reported by Kevin Joensen <kevin@baldur.dk> from Baldur Security.

Fixed: pmg-api >= 8.2.7 (PMG 8.x), pmg-api >= 9.0.3 (PMG 9.x)

References: Advisories PSA-2026-00002-1, PSA-2026-00003-1, and PSA-2026-00004-1 all address similar issues in other Proxmox projects.



ProxmoxSecurityAdvisory
Proxmox Staff Member

Staff member

Feb 17, 2026 #12

Subject: PSA-2026-00005-1: Bypass of mail filters through confusion of the MIME Parser

Advisory date: 2026-02-17

Packages: pmg-api, libmime-tools-perl

Details: The parser initially processing e-mails for further analysis was set to not cause an error on non-standard and ambiguous information in the 'Content-Type' header:
- multiple occurrences of a 'Content-Type' header
- mulitple boundary parameters for multipart messages
- backslash as part of the boundary parameter for multipart messages
- non-printable and non ASCII characters as part of the boundary parameter for multipart messages

Accepting such messages can lead to unwanted content to be delivered to a mailbox, where the mail client interprets the ambiguous information differently. This made it effectively possible to construct a mail with an unwanted attachment, passing the filter, which was then accessible to the end-user.

The issue was addressed by rejecting mails with ambiguous content, and other errors in their structure by default. The default setting can be changed with the `accept-broken-mime` setting in the `pmg.conf` configuration file to ensure compatibility with trusted systems which send out mails with ambiguous structure. If `accept-broken-mime` is enabled, mails which have problematic content are logged and additionally a `X-Proxmox-Broken-Message` header is added, which can used for matching in the rule system (through a 'Match-Field' What Object).

This issue was initially reported by Artem Danilov of Positive Technologies.

Additionally, an issue with the treatment of an empty boundary parameter was identified and fixed in the perl MIME::Tools package. We'd like to thank Dianne Skoll <dianne@skoll.ca>, for reviewing the fix and cooperating with us.

Fixed:
- Proxmox Mail Gateway 8: pmg-api >= 8.2.10, libmime-tools-perl >= 5.515-1+pmg1~bpo12+1
- Proxmox Mail Gateway 9: pmg-api >= 9.0.6, libmime-tools-perl >= 5.515-1+pmg1



ProxmoxSecurityAdvisory
Proxmox Staff Member

Staff member

Mar 13, 2026 #13

Subject: PSA-2026-00010-1: "Crackarmor" apparmor vulnerabilities

Advisory date: 2026-03-13

Packages: proxmox-kernel-*

Details:

Qualys discovered several vulnerabilities in the AppArmor LSM (Linux Security Module) code of the Linux kernel, which are being referred to as "Crackarmor".

All of the vulnerabilities require unprivileged local user access. The impact of these

vulnerabilities ranges from denial of service, kernel memory information leak, removing security controls, local privilege escalation to root user to potential container escapes.

Refer to the upstream advisories linked below for more details.

Fixed:
- proxmox-kernel-6.8.12-20-pve(-signed) (Bookworm based releases)
- proxmox-kernel-6.14.11-6-bpo12-pve(-signed) (Bookworm based releases)
- proxmox-kernel-6.14.11-6-pve(-signed) (Trixie based releases)
- proxmox-kernel-6.17.13-2-pve(-signed) (Trixie based releases)

References:
- https://cdn2.qualys.com/advisory/2026/03/10/crack-armor.txt (Qualys advisory)
- https://ubuntu.com/security/vulnerabilities/crackarmor (Ubuntu Security Team advisory)



ProxmoxSecurityAdvisory
Proxmox Staff Member

Staff member

Aug 3, 2026 #14

Subject: PSA-2026-00033-1: Authenticated Remote Code Execution via custom_check_path setting

Advisory date: 2026-08-03

Packages: pmg-api

Details:

The custom_check_path setting could be set by any user with 'Administrator' role. This script is executed for every mail received, with the path to the mail contents as argument, potentially leading to a privilege escalation to `root` for pmg-api versions < 9.1.0, or the local `pmg-smtp-filter` user for pmg-api >= 9.1.0.

As uploading scripts is not part of the PMG API, the issue only allows executing pre-existing executables on the system, without controlling their enviroment or arguments, which effectively limits the usefulness of the missed permission check.

To prevent exploiting the issue the `custom_check_path` setting was changed to be only settable by `root@pam`.

Fixed in:
- pmg-api >= 9.1.1 (PMG 9.x)
- pmg-api >= 8.2.12 (PMG 8.x)

References:

This issue was discovered internally.



ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Sep 21, 2026 #15

Subject: PSA-2026-00048-1: PMG: XSS in filename display in attachment quarantine

Advisory date: 2026-09-21

Packages: pmg-gui

Details:

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

Fixed in:
- pmg-gui >= 5.2.3

Last edited: Sep 21, 2026



ProxmoxSecurityAdvisory
Proxmox Staff Member
Staff member

Sep 21, 2026 #16

Subject: PSA-2026-00049-1: PMG: Bypass of mail filters by crafted boundary parameters

Advisory date: 2026-09-21

Packages: pmg-api, libmime-tools-perl

Details:

Certain problematic strings used as `Content-Type` boundaries were not covered by the fixes for PSA-2026-00005-1. With a fitting boundary the parser could be tricked into treating a malicious attachment as epilogue to a multipart message and skipping the checks on the part.

Some mail user agents display such parts hidden in the epilogue as attachments, potentially exposing users to unwanted and dangerous content.

This issue was privately reported by Artem Danilov of Positive Technologies.

Fixed in:
- libmime-tools-perl >= 5.515-1+pmg2

References:
- PSA-2026-00005-1 was about a similar issue.



ProxmoxSecurityAdvisory
Proxmox Staff Member

Staff member

Oct 7, 2026 #17

Subject: PSA-2026-00063-1: PMG: Administrator to root privilege escalation via http_proxy configuration setting

Advisory date: 2026-10-07

Packages: pmg-api

Details:

Insufficient input validation for the `http_proxy` configuration setting allowed an attacker with Administrator role to inject arbitrary contents into the `/etc/apt/apt.conf.d/76pmgproxy` configuration file. In particular, an `APT::Update::Pre-Invoke` setting is executed as the root user during package update, allowing for arbitrary command execution as root.

The issue was addressed by restricting setting `http_proxy` to `root@pam` and by parsing the setting more strictly.

This issue was privately reported by: Vo Van Phuc - VNPT Cyber Immunity (VCI)
Diem - VNPT Cyber Immunity (VCI)

Fixed in:
- pmg-api >= 9.1.3



ProxmoxSecurityAdvisory
Proxmox Staff Member

Staff member

Oct 7, 2026 #18

Subject: PSA-2026-00064-1: PMG: Administrator to root privilege escalation via private keys in backup

Advisory date: 2026-10-07

Packages: pmg-api

Details:

A user with `Administrator` role could create and download a backup, which includes the private key material for the API server. This can be used to forge a session as the `root@pam` user.

Since the host where a backup is being restored already has its own set of authentication keys, and any derived values are only valid temporarily, not including them in the backup both improves post-restore behaviour of the system, and

prevents leaking of the keys used by the backed-up system.

The issue was privately reported by Điềm from VNPT-VCI.

Fixed in:
- pmg-api >= 9.1.3



ProxmoxSecurityAdvisory
Proxmox Staff Member

Staff member

Oct 7, 2026 #19

Subject: PSA-2026-00065-1: PMG: Bypass DMARC check by spoofed envelope sender header

Advisory date: 2026-10-07

Packages: pmg-api

Details:

Adding a `X-Proxmox-Envelope-From` header to a mail confuses `pmg-smtp-filter` into using the mail-address there, instead of the actual envelope sender for the DMARC alignment check. Sending a mail with valid SPF result from one domain can yield a pass result for the strict DMARC policy of a different domain, effectively bypassing DMARC.

The issue is addressed, by passing the envelope sender address directly to SpamAssassin instead of by adding a `X-Proxmox-Envelope-From` header before parsing. This also modifies the template for SpamAssassin's `local.cf` configuration file. If you have a modified `/etc/pmg/templates/local.cf.in` make sure to adapt it to the removal of `envelope_sender_header X-Proxmox-Envelope-From`.

The issue was privately reported by Gabriele Caniglia, NetRelay <proxmox@netrelay.it>.

Fixed in:
- pmg-api >= 9.1.3

Not open for further replies.

Share:

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

Quick Navigation

Home
Get Subscription
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.