

FREE CVE ADVISORY · TLP:CLEAR

BeyondTrust Remote Support zero-day is being exploited (CVE-2026-102764)

CVE-2026-102764 is a critical flaw (CVSS 3.1: 9.8) in BeyondTrust Remote Support, the remote-support appliance formerly called Bomgar.

SEVERITY

CRITICAL

CVSS 3.1

9.8

EXPLOITED

Yes

FIX AVAILABLE

Yes

01

At a glance

SEVERITY	CRITICAL CVSS 3.1 9.8
EXPLOITED IN THE WILD	Yes. In CISA's Known Exploited Vulnerabilities catalog since 16 October 2026
FIX AVAILABLE	Yes: patch BT26-05-RS for self-hosted 24.3.1 to 26.2.3 (older versions upgrade first); SaaS tenants patched by BeyondTrust on 9 October 2026
PATCH DEADLINE	19 October 2026 for US federal civilian agencies (CISA BOD 22-01)
WHAT AN ATTACKER NEEDS	Network, no privileges, no user interaction
EPSS	0.6% chance of exploitation in 30 days, 48th percentile (2026-10-16)
AFFECTED	BeyondTrust Remote Support (formerly Bomgar) 26.2.3 and earlier, self-hosted; SaaS tenants already patched

02

What is happening

CVE-2026-102764 is a critical flaw (CVSS 3.1: 9.8) in BeyondTrust Remote Support, the remote-support appliance formerly called Bomgar. Internal components did not check where the messages they received came from, so an attacker who can reach the appliance over the network, with no account, can make it perform file operations: in practice, upload files to it. Google's Threat Intelligence Group (GTIG) reports that a suspected China-nexus espionage actor it tracks as ARMORY CASTLE (formerly UNC5221) used the flaw as a zero-day from late August 2026 to take root on an appliance, dump every credential it stored and open sessions into the systems it managed.

A patch exists: **BT26-05-RS**, for self-hosted versions 24.3.1 to 26.2.3; older versions must upgrade first. BeyondTrust patched all SaaS tenants on 9 October 2026. CISA added the flaw to its Known Exploited Vulnerabilities catalog on 16 October and gave US federal civilian agencies until **19 October 2026**.

Patching closes the door; it does not evict anyone already inside. GTIG's advice is blunt: any appliance that was reachable from the internet on a vulnerable version during the exploitation window should be treated as potentially compromised until it has been reviewed.

03

Who is affected

Every organisation running **BeyondTrust Remote Support** (formerly Bomgar) **self-hosted** at version **26.2.3 or earlier**: that is all supported versions, according to CISA and GTIG. Appliances whose web interface is reachable from the internet are the most exposed, because the flaw needs no credentials.

SaaS customers: BeyondTrust applied the patch to all Remote Support SaaS tenants on 9 October 2026, so there is nothing to install. The hunting advice below still applies to the accounts, roles and sessions you control.

Keep in mind what this appliance holds. Remote Support brokers access to endpoints and stores credentials for them; GTIG describes the impact as access to every credential the appliance stores or brokers, and the actor used stolen administrator credentials to start sessions into internal systems. The blast radius is not the appliance. It is everything the appliance can reach.

04

Do this now

- 01 Patch today.** Self-hosted appliances on 24.3.1 to 26.2.3: apply **BT26-05-RS** from the `/appliance` interface, as described in BeyondTrust advisory BT26-05. Older than 24.3.1: upgrade to a supported version first, then apply the patch. SaaS tenants were patched by BeyondTrust on 9 October 2026.
- 02 Preserve before you touch anything.** If the appliance was reachable from the internet on a vulnerable version at any time since late August 2026, treat it as potentially compromised. Snapshot the virtual appliance with its memory (or image a physical one) and collect the logs that live off the box: reverse proxy, WAF, perimeter firewall, your SIEM. The actor deleted the appliance's own logs throughout the intrusion.
- 03 Hunt with the indicators below.** The fastest checks: a root-owned SUID copy of `/bin/sh` at `/usr/bin/dbus-authd`; the boot script `/home/bomgar/sbin/post_boot.d/zz-root-persist`; a `webskd3` backend or `/uidchanarge` path in `/ns/config/haproxy.conf`; `/tmp/ingredi_ws`; unknown `.php` files under the site's Laravel public directory; and `user_changed` events in `/login` that raised an account's Jump Item or Team roles.
- 04 If you find any of it, rebuild, do not clean.** Isolate the appliance, redeploy it from a clean image, apply the patch, then rotate every credential the appliance stored or injected, in dependency order, revoke all active support sessions and review new MFA registrations on privileged accounts. Rotate after the rebuild, not before: new secrets handed to a compromised appliance are stolen too.
- 05 Cut the exposure.** Restrict `/login` and `/appliance` to trusted networks or a VPN, require SAML single sign-on with phishing-resistant MFA for administrators, and forward syslog and session events to your SIEM so the next log deletion leaves a visible gap. US federal civilian agencies must remediate by **19 October 2026** (CISA BOD 22-01); everyone else should treat that date as the benchmark.

05

Vulnerability details

NVD describes the weakness as follows: "The vulnerability exists within internal components of BeyondTrust's Remote Support product. The components did not adequately validate the origin of the messages it received. Under the right conditions, this could allow an attacker to perform file operations on the appliance." It is classified as **CWE-290, Authentication Bypass by Spoofing**. GTIG puts the result more plainly: arbitrary file upload by an unauthenticated remote attacker, "which can lead to host-level control and access to every credential the appliance stores or brokers".

NVD scores it **9.8 Critical** on CVSS 3.1 (`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` : network-reachable, low complexity, no privileges, no user interaction, full impact on confidentiality, integrity and availability) and 9.3 Critical on CVSS 4.0. The EPSS score on 16 October 2026 was 0.6% (48th percentile): EPSS lags behind newly exploited flaws, and the KEV listing and GTIG's incident evidence are the stronger signals.

Who is behind it. GTIG attributes the zero-day exploitation, and the SAWFLY web shell and BARECLAW tunneler found on the appliance, to **ARMORY CASTLE**, a suspected PRC-nexus espionage actor formerly tracked as UNC5221 (CrowdStrike: WARP PANDA), active since at least October 2023 and known for zero-days in edge devices, including the Ivanti Connect Secure flaws of early 2024. GTIG gives no victim count or sector breakdown, and warns that after disclosure the group has in the past moved to widespread, opportunistic exploitation. CISA records known ransomware use as "Unknown".

The fix. BeyondTrust advisory BT26-05 (15 October 2026) provides patch **BT26-05-RS** for self-hosted Remote Support 24.3.1 to 26.2.3; versions older than 24.3.1 have to be upgraded to a supported version before the patch can be applied. All SaaS tenants were patched on 9 October 2026. The vendor's advisory and its knowledge-base article KB0024066 (customer login) hold the exact procedure; the patch facts here are as published by CISA, the Canadian Centre for Cyber Security and GTIG.

CVE	CVSS 3.1	WEAKNESS	EXPLOITED
CVE-2026-102764 BeyondTrust Remote Support Authentication Bypass by Spoofing Vulnerability	9.8 CRITICAL CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CWE-290	Yes (CISA KEV)

PRODUCT	AFFECTED VERSIONS	FIXED IN
BeyondTrust Remote Support, self-hosted	26.2.3 and earlier (all supported versions)	Patch BT26-05-RS on 24.3.1 to 26.2.3; older versions upgrade first
BeyondTrust Remote Support, SaaS	All tenants until 9 October 2026	Patched by BeyondTrust on 9 October 2026

06

How an attack works

STEP	WHAT HAPPENS	ATT&CK
Initial access	POST requests to a crafted path (/app_84304470%2Ephp) exploit the origin-validation flaw to write files to the appliance. No account is needed.	T1190
Web shell	About 11 minutes later the SAWFLY PHP web shell (mangoapi.php) appears under the site's Laravel public directory. It answers HTTP 404 unless the request carries its _c94mfe parameter, then RC4-decrypts the payload and runs it with eval() .	T1505.003
Root	/bin/sh is copied to /usr/bin/dbus-authd , owned by root with the SUID bit set: a persistent root shell.	T1548.001
Credential theft	The appliance's own /ns/sbin/bt-secrets CLI dumps the vault (bt-secrets get ... vault); the actor then deletes /home/bomgar/log/bt-secrets.log .	T1555

STEP	WHAT HAPPENS	ATT&CK
Persistence	A boot script, <code>/home/bomgar/sbin/post_boot.d/zz-root-persist</code> , appends a passwordless-sudo line for the site service account to <code>/ns/config/sudoers.template</code> and rebuilds <code>/etc/sudoers</code> with <code>bt-sysconfig</code> . It survives reboots and configuration resets.	T1037, T1548.003
Covering tracks	Appliance logs deleted throughout the intrusion: <code>/ns/log/auth.log</code> , <code>ssl.log</code> , <code>http-access.log</code> , <code>/var/log/messages</code> , <code>/tmp/sshauth.*</code> and the site's httpd logs.	T1070.002
Lateral movement	With stolen administrator credentials the actor logs into <code>/login</code> , raises the account's Jump Item and Team roles from No Access to Administrator (a <code>user_changed</code> event), starts support sessions to internal endpoints with full file-system access and pulls documents out through the file-transfer service.	T1078, T1021, T1005
Tunnel	BARECLAW (<code>/tmp/ingredi_ws</code>), a SOCKS5-over-WebSocket proxy, listens on <code>127.0.0.1:19800</code> ; an added <code>webskd3</code> backend in <code>/ns/config/haproxy.conf</code> exposes it to the internet at the path <code>/uidchanarge</code> .	T1090, T1572

07

Indicators and detection

TYPE	INDICATOR (DEFANGED)	WHAT IT IS
path	<code>/usr/bin/dbus-authd</code>	SUID root copy of <code>/bin/sh</code>
path	<code>/home/bomgar/sbin/post_boot.d/zz-root-persist</code>	boot-time sudoers persistence
path	<code>/ns/config/haproxy.conf</code>	added ACL <code>wswws / backend webskd3 → 127.0.0.1:19800</code>
path	<code>/tmp/ingredi_ws</code>	BARECLAW tunneler
sha256	<code>1f19b9a27d79c11bda00a1e8faf74a7fdd683d38ccf1b60df2fd0307e3aa462</code>	<code>ingredi_ws</code> (BARECLAW)
file	<code>mangoapi.php</code>	SAWFLY web shell, under <code>.../ingredi/app/laravel/public/</code>
sha256	<code>dc14e215269a93fdb4c1a80b984c23faf7af0911c6dbb85309796a6f2ae95fb</code>	<code>mangoapi.php</code> (SAWFLY)
path	<code>/app_84304470%2Ephp</code>	request path used to stage the web shell

TYPE	INDICATOR (DEFANGED)	WHAT IT IS
path	/uidchanarge	WebSocket path HAProxy forwards to BARECLAW
yara	G_Hunting_Webshell_SAWFLY_1	GTIG YARA rule
yara	G_Hunting_Backdoor_BARECLAW_1	GTIG YARA rule

Where to look

- /login audit events: `user_changed` entries that raise Jump Item or Team roles; `user_added`, `api_account` or `security_provider` events with no change ticket; changes to syslog or outbound event destinations.
- /login successes from residential or commercial VPN address space, and administrative logins outside business hours.
- Session records: file-transfer events, and sessions started by accounts whose roles changed.
- Web server requests to unknown `.php` paths, and WebSocket upgrades from addresses that are not your support staff or endpoints.
- Gaps in syslog forwarding: GTIG calls an interruption bounded by a single session a strong indicator of tampering.
- GTIG lists no IP addresses or domains for this activity and points to logins from VPN address space instead, so block-lists will not help; the host artefacts above will.
- CISA asks for network and memory forensics on suspected appliances: the on-appliance logs cannot be trusted.

08

After the first 24 hours

This week

- Confirm the patch or upgrade landed on every Remote Support appliance, including standby, test and disaster-recovery units, and that automatic updates are on where you want them.
- Compare the /login configuration (accounts, roles, Jump Item policies, API accounts, security providers, syslog targets) with a baseline from before late August 2026, and reset default Jump Item roles to No Access.
- Rotate what the appliance could reach even if you found nothing: credentials it stores or injects, API keys, service accounts; revoke standing support sessions.
- Tell your incident-response retainer or MSSP that you run this product. GTIG expects the group to turn opportunistic now that the flaw is public.

Longer term

- Keep remote-support and remote-access appliances off the open internet where the business allows: VPN or allow-listed access, SAML SSO with phishing-resistant MFA, admin interfaces on trusted networks only.
- Ship appliance syslog and session events to a SIEM you control, and alert on gaps: this actor deletes logs as a routine.

- Put remote-access products on a 72-hour patch track: CISA's KEV deadlines for this class of product are consistently the shortest, and edge devices are where this actor lives.
- Treat every appliance that brokers credentials as Tier 0: segment it, monitor it, and know how to rebuild it from a clean image in a day.

09

Timeline

2026-08-29	First known exploitation, as a zero-day (BeyondTrust's timeline, as reported by The Hacker News; GTIG dates it to late August 2026)
2026-10-09	BeyondTrust applies the patch to all Remote Support SaaS tenants
2026-10-15	BeyondTrust publishes advisory BT26-05 and patch BT26-05-RS; GTIG publishes its ARMORY CASTLE report; NVD publishes the CVE record
2026-10-16	CISA adds the CVE to the Known Exploited Vulnerabilities catalog and publishes an alert; the Canadian Centre for Cyber Security publishes AL26-025
2026-10-17	This advisory
2026-10-19	CISA remediation due date for US federal civilian agencies (BOD 22-01)

10

References

Vendor advisory BT26-05 (BeyondTrust)

<https://www.beyondtrust.com/trust-center/security-advisories/bt26-05>

Vendor blog: ARMORY CASTLE and BT26-05, what security teams need to know

<https://www.beyondtrust.com/blog/entry/bt26-05>

BeyondTrust knowledge-base article KB0024066 (customer login)

https://beyondtrustcorp.service-now.com/csm?id=csm_kb_article&sysparm_article=KB0024066

Google Threat Intelligence Group: ARMORY CASTLE exploits BeyondTrust (15 October 2026)

<https://cloud.google.com/blog/topics/threat-intelligence/armory-castle-exploits-beyondtrust>

CISA alert: CISA urges patching critical vulnerability in BeyondTrust Remote Support (16 October 2026)

<https://www.cisa.gov/news-events/alerts/2026/10/16/cisa-urges-patching-critical-vulnerability-beyondtrust-remote-support>

CISA Known Exploited Vulnerabilities catalog entry

https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-102764

CISA BOD 26-04 implementation guidance

<https://www.cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk>

Canadian Centre for Cyber Security alert AL26-025 (16 October 2026)

<https://www.cyber.gc.ca/en/alerts-advisories/al26-025-critical-vulnerability-impacting-beyondtrust-remote-support-cve-2026-102764>

NVD record

<https://nvd.nist.gov/vuln/detail/CVE-2026-102764>

EPSS score (FIRST)

<https://api.first.org/data/v1/epss?cve=CVE-2026-102764>

BeyondTrust docs: securing a self-hosted appliance

<https://docs.beyondtrust.com/rs/docs/on-prem-security>

The Hacker News: China-linked hackers exploited BeyondTrust zero-day (16 October 2026)

<https://thehackernews.com/2026/10/china-linked-hackers-exploited.html>

11**Sources and method**

Google Threat Intelligence Group report of 15 October 2026 (attack chain, indicators, attribution); CISA alert and KEV entry of 16 October 2026 (affected versions, patch availability, recommended actions); Canadian Centre for Cyber Security alert AL26-025 of 16 October 2026 (patch name and SaaS patch date, relaying BeyondTrust advisory BT26-05); NVD record for CVE-2026-102764, last modified 2026-10-17 (description, CWE, CVSS); FIRST EPSS of 2026-10-16; The Hacker News of 16 October 2026 (the 29 August date only).

Every fact above comes from those sources. CVSS scores are computed from the published vector. Indicators are defanged. Nothing is added from memory or guesswork; where the sources are silent, this advisory says so. Recommendations are Cyberphobia's own guidance.

ABOUT

Don't fear cybersecurity. Master it.

Cyberphobia publishes free, practical security content: short videos, step-by-step guides and these advisories, written by a cybersecurity executive leader who runs security programs and oversees SOC operations. Advisories cover what is being exploited right now and what to do about it this week.

Instagram, TikTok, YouTube, Facebook: [@cyberphobiatv](#)

LinkedIn: [abuyv](#)

All advisories: cyberphobia.net/advisories

Newsletter: cyberphobia.net/newsletter

Sharing. TLP:CLEAR: recipients can spread this to the world, there is no limit on disclosure. Licensed CC BY 4.0: share and adapt it, credit Cyberphobia.

Accuracy. Facts come only from the sources named in the advisory, as published on the date shown; CVSS scores are computed from the published vectors. Vendors and CISA update their guidance, so check the references for the current state.

No warranty. This advisory is general guidance provided free of charge, as is. Test every change in your own environment. It is not a substitute for your vendor's instructions or your own risk assessment.