Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-1731: Active Exploitation of BeyondTrust WebSocket RCE

Date of Publication	Admiralty Code	TA Number
February 16, 2026	A1	TA2026044

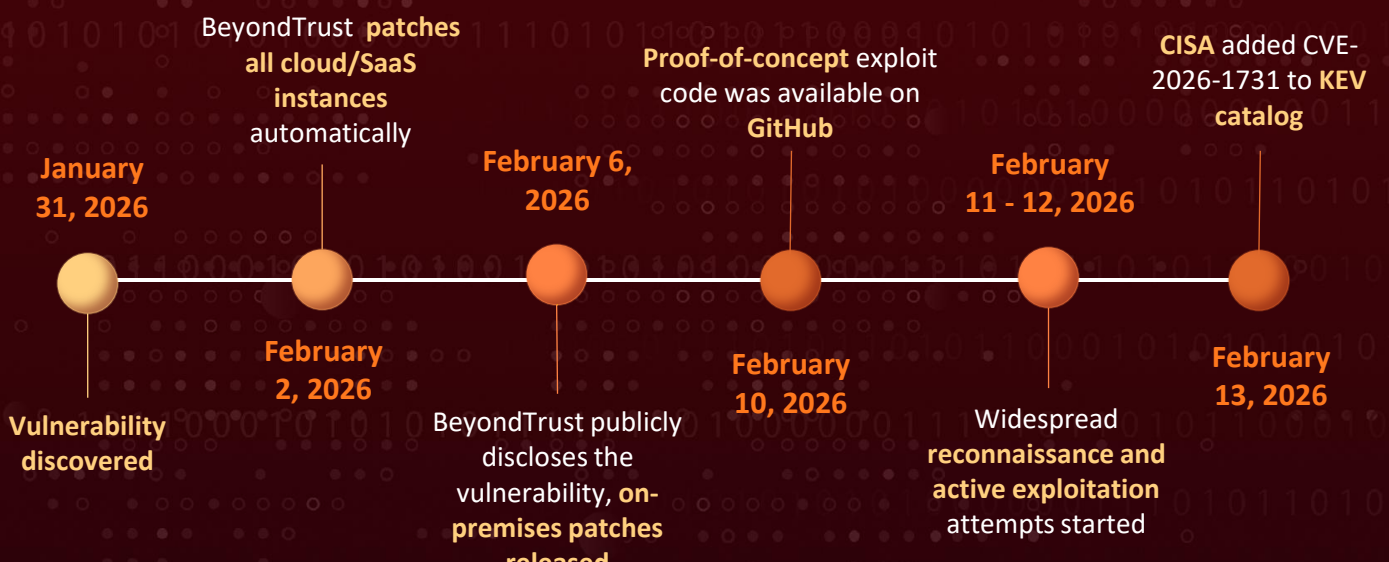
Summary

First Seen: January 31, 2026
Affected Products: BeyondTrust Remote Support (RS), BeyondTrust Privileged Remote Access
Impact: CVE-2026-1731 is a critical unauthenticated remote code execution vulnerability in BeyondTrust Remote Support and Privileged Remote Access appliances caused by an OS command injection flaw in a WebSocket endpoint. It enables full system compromise without authentication and is actively exploited in the wild. Organizations running affected self-hosted versions should immediately upgrade to patched releases and assess for potential compromise.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-1731	BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability	BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA)	✗	✓	✓

Exploitation Timeline



Vulnerability Details

#1

CVE-2026-1731 is a critical, unauthenticated remote code execution (RCE) vulnerability affecting BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) products. The flaw stems from an OS command injection vulnerability (CWE-78) that allows attackers to execute arbitrary system commands without authentication or user interaction by sending specially crafted requests to a WebSocket-accessible endpoint. The vulnerability has received a CVSSv4 score of 9.9, reflecting the risk of full system compromise, unauthorized access, data exfiltration, and lateral movement within enterprise environments.

#2

The vulnerability impacts Remote Support versions 25.3.1 and earlier and Privileged Remote Access versions 24.3.4 and earlier in self-hosted deployments. CVE-2026-1731 shares similarities with CVE-2024-12356, a previously exploited zero-day affecting related WebSocket functionality in BeyondTrust appliances. Because these products provide remote administration and privileged access capabilities, successful exploitation can grant attackers high-value control over sensitive infrastructure. Security researchers have estimated that thousands of on-premises instances were internet-facing and potentially exposed at the time of disclosure. SaaS instances were patched automatically on February 2, 2026, while on-premises users must apply updates manually.

#3

Public disclosure occurred on February 6, 2026, and proof-of-concept (PoC) exploit code became available soon after that. Widespread scanning and exploitation attempts were observed shortly thereafter. Threat actors targeted exposed instances, abused vulnerable endpoints to execute system commands, and in some cases deployed remote monitoring and management (RMM) tools to establish persistence. Researchers also observed probing of non-standard ports, suggesting attackers anticipated defensive reconfiguration of exposed services.

#4

Organizations running affected versions should immediately upgrade to the patched releases (Remote Support 25.3.2 or later and Privileged Remote Access version 25.1.1 or later). Additional defensive measures include restricting external exposure of management interfaces, monitoring for anomalous WebSocket activity and unexpected process execution from the web service context, and conducting compromise assessments. Given the low attack complexity, public exploit availability, and confirmed active exploitation, CVE-2026-1731 should be treated as a high-priority remediation item for security and IT operations teams.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-1731	BeyondTrust Remote Support: Before 25.3.2 BeyondTrust Privileged Remote Access: Before 25.1.1	cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*:*:* cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Apply Patches Immediately: Self-hosted users running BeyondTrust Remote Support versions v21.3 through 25.3.1 must upgrade to version 25.3.2 or later without delay. Self-hosted Privileged Remote Access users running versions v22.1 through 24.x must upgrade to version 25.1.1 or later. Cloud and SaaS users were automatically patched by BeyondTrust as of February 2, 2026, and should verify with BeyondTrust that their instances reflect the updated version.

Verify Automatic Update Subscription: Organizations running self-hosted BeyondTrust deployments should confirm whether their instances are subscribed to automatic updates. If automatic updates are not enabled, manual patch application is required. Ensure that the patch deployment process is documented and that successful installation is validated through version verification.

Restrict Network Exposure of BeyondTrust Instances: Where feasible, limit external access to BeyondTrust Remote Support and Privileged Remote Access instances by placing them behind VPN gateways, firewalls, or zero-trust network access solutions. Attackers are probing both standard (port 443) and non-standard ports, indicating that relying on port obscurity alone is insufficient. Only authorized administrators and support personnel should have network-level access to these services.

Conduct Compromise Assessment: Review logs for anomalous WebSocket activity, unexpected command execution, suspicious child processes spawned by web services, and unauthorized administrative sessions. Investigate for newly created accounts, modified configurations, or deployed RMM tools.

Enhance Monitoring & Detection: Given the observed post-exploitation behavior, organizations should specifically monitor for the deployment of unauthorized RMM tools across their environment, unexpected PSExec execution across multiple hosts, and Impacket-based SMBv2 session activity. Endpoint detection and response (EDR) solutions should be tuned to alert on these behaviors.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Reconnaissance	T1595: Active Scanning	T1595.002: Vulnerability Scanning
Discovery	T1018: Remote System Discovery	
Lateral Movement	T1021: Remote Services	
Command and Control	T1219: Remote Access Software	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
Privilege Escalation	T1068: Exploitation for Privilege Escalation	

Patch Link

https://www.beyondtrust.com/trust-center/security-advisories/bt26-02

References

https://www.hacktron.ai/blog/cve-2026-1731-beyondtrust-remote-support-rce

https://www.beyondtrust.com/trust-center/security-advisories/bt26-02

https://www.greynoise.io/blog/reconnaissance-beyondtrust-rce-cve-2026-1731

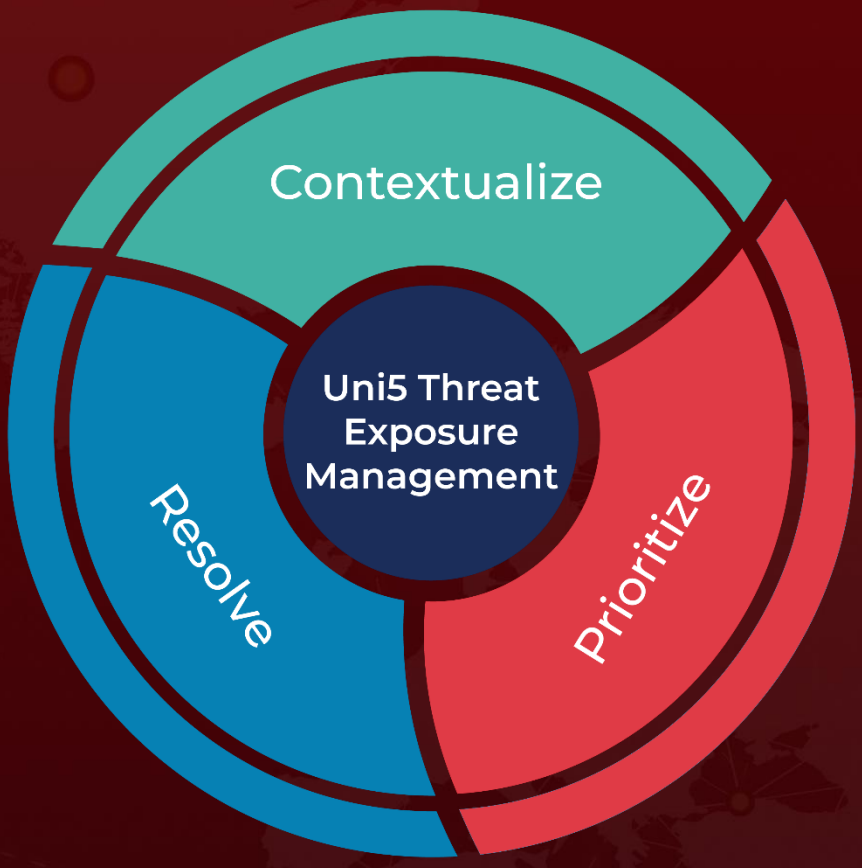
https://www.rapid7.com/blog/post/etr-cve-2026-1731-critical-unauthenticated-remote-code-execution-rce-beyondtrust-remote-support-rs-privileged-remote-access-pra/

https://hivepro.com/threat-advisory/postgresql-flaw-cve-2025-1094-joins-beyondtrust-zero-day-in-stealthy-attacks/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 16, 2026 • 06:30 AM

More at www.hivepro.com