CYBER ADVISORY

Wednesday, February 18, 2026

CSIC-ADVISORY-202602-A-010

BeyondTrust OS Command Injection Vulnerability

Unauthorized Access	Data Exfiltration	Proof-of-Concept	Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has identified a critical vulnerability impacting BeyondTrust Remote Support (RS) and Privilege Remote Access (PRA) platforms. CVE-2026-1731 carries a CVSS 3.1 score of 9.8.[1] Successful exploitation could allow an unauthenticated remote attacker to execute operating system commands in the context of the site user and may lead to system compromise, including unauthorized access, data exfiltration, and service disruption.[2] CVE-2026-1731 has been confirmed to be exploited, and a proof-of-concept has been posted.

***Analyst Comment**: BeyondTrust has observed CVE-2026-1731 currently being exploited in the wild. There has also been a surge of reconnaissance for vulnerable, public-facing devices which very likely indicate that increased exploitation attempts on unpatched systems will follow.*

The vendor has issued a security advisory with patching and mitigation instructions.

The Cal-CSIC recommends immediately following the vendor's guidance in mitigation and patching. Self-hosted customers need to manually update to the latest versions of BeyondTrust's Remote Support and Privileged Remote Access.[3] For further information on BeyondTrust's security advisory and analysis please use this link:

Security Advisory

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

Affected Product:

Product Name	Affected Version	Solution
BeyondTrust Remote Support	25.3.1 and prior	Patch BT26-02-RS Remote Support 25.3.2 and greater
BeyondTrust Privileged Remote Access	24.3.4 and prior	Patch BT26-02-PRA (v22.1-24.X) Privileged Remote Access 25.1 and greater

References

[1] NVD; "CVE-2026-1731 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-1731; accessed 18 February 2026
[2] BeyondTrust; "BT26-02"; https://www.beyondtrust.com/trust-center/security-advisories/bt26-02; accessed 18 February 2026
[3] Greynoise; "BeyondTrust RCE (CVE-2026-1731): What We're seeing in the Wild"; https://www.greynoise.io/blog/reconnaissance-beyondtrust-rce-cve-2026-1731; accessed 18 February 2026