

BeyondTrust Remote Support Authentication Bypass Vulnerability Requires Immediate Action



BeyondTrust Remote Support contains an authentication bypass vulnerability allowing remote attackers to perform file operations on the appliance, requiring immediate vendor mitigations.

- CVE-2026-102764 affects BeyondTrust Remote Support with an authentication bypass by spoofing vulnerability
- Remote attackers can exploit the flaw to perform file operations on the appliance
- Vendor mitigations must be applied immediately or product use discontinued if patches unavailable
- Organizations must evaluate internet exposure of affected assets and follow risk-based patching guidance
- CISA references BOD 26-04 prioritization framework with federal deadline of 19 October 2026

Vulnerability Overview

BeyondTrust Remote Support, a widely deployed remote access solution, contains a critical **authentication bypass by spoofing** vulnerability tracked as CVE-2026-102764. The flaw enables remote attackers to circumvent authentication controls and perform unauthorized file operations directly on the appliance. This represents a significant risk for organizations relying on the platform for privileged remote access and support workflows.

The vulnerability's exploitation does not require prior authentication, making it particularly dangerous for internet-facing deployments. Attackers successfully exploiting this weakness could gain unauthorized access to sensitive files, potentially compromising the integrity and confidentiality of systems managed through the platform.

Required Response Actions

CISA has issued guidance requiring organizations to apply vendor-supplied mitigations immediately. Where patches or mitigations are unavailable, organizations must discontinue use of the affected product. The advisory references CISA's Binding Operational Directive 26-04, which establishes a risk-based framework for prioritizing security updates, with a federal compliance deadline of 19 October 2026.

Organizations must conduct forensics triage in accordance with CISA's published requirements to identify potential compromise. Particular attention should be paid to assets with internet exposure, as these face elevated risk.

Implications for Saudi Institutions

Regulated entities in the Kingdom using BeyondTrust Remote Support for privileged access management should treat this as a priority incident response matter. The vulnerability's potential to bypass authentication controls directly conflicts with access control requirements under multiple Saudi regulatory frameworks. Immediate inventory of affected systems and coordination with BeyondTrust for mitigation guidance is essential.

What to do now

1. Immediately inventory all BeyondTrust Remote Support deployments across your organization, noting version numbers and internet exposure status
2. Contact BeyondTrust support to obtain and apply vendor-supplied patches or mitigations for CVE-2026-102764 without delay
3. If mitigations are unavailable, isolate affected systems from the internet or discontinue use until patches are released
4. Conduct forensics triage on all BeyondTrust appliances to identify indicators of compromise or unauthorized file access

5. Review access logs for anomalous authentication patterns or file operations that may indicate exploitation attempts
6. Update incident response procedures and notify relevant stakeholders including NCA-CERT if compromise is detected or suspected