An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2607080262

# NCSC Advisory

## Critical Vulnerabilities exist in BeyondTrust Remote Support and Privileged Remote Access

CVE-2026-40138 and CVE-2026-40139

**8th, July 2026**

**STATUS: TLP:CLEAR**

**Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.**

**For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.**

# Description

**CVE ID:** CVE-2026-40138

**Published:** 2026-07-06

**Vendor:** BeyondTrust

**Product:** Remote Support and Privileged Remote Access

**CVSS Score[1]:** 9.2

# Products Affected

| Product | Version |
|---|---|
| Remote Support | 0 <= 25.3.2 |
| Privileged Remote Access | 0 <= 25.3.2 |

# Impact

A critical pre-authentication vulnerability exists in the authentication subsystem of BeyondTrust Remote Support and Privileged Remote Access. Improper validation of authentication data may allow a network-positioned attacker to bypass access controls and gain unauthorized access to the appliance, including accounts with elevated privileges. Exploitation requires a specific authentication configuration to be enabled.

Common Weakness Enumeration (CWE)[2]: CWE-287 Improper Authentication

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

# Description

**CVE ID:** CVE-2026-40139

**Published:** 2026-07-06

**Vendor:** BeyondTrust

**Product:** Remote Support

**CVSS Score**[4]: 9.2

# Products Affected

| Product | Version |
|---|---|
| Remote Support | 0 <= 25.3.2 |

# Impact

A critical pre-authentication vulnerability exists in the authentication subsystem of BeyondTrust Remote Support. Improper processing of authentication requests may allow an unauthenticated remote attacker to bypass access controls and gain unauthorized access to the appliance, including accounts with elevated privileges. Exploitation requires a specific authentication configuration to be enabled.

Common Weakness Enumeration (CWE)[5]: CWE-287 Improper Authentication

Known Exploited Vulnerability (KEV) catalog[6]: No

Used by Ransomware Operators: N/A

[4] https://www.first.org/cvss/

[5] https://cwe.mitre.org

[6] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

# Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from BeyondTrust.

CVE-2026-40138:

- https://nvd.nist.gov/vuln/detail/CVE-2026-40138
- https://www.cve.org/CVERecord?id=CVE-2026-40138
- https://www.beyondtrust.com/trust-center/security-advisories/bt26-03

CVE-2026-40139:

- https://nvd.nist.gov/vuln/detail/CVE-2026-40139
- https://www.cve.org/CVERecord?id=CVE-2026-40139
- https://www.beyondtrust.com/trust-center/security-advisories/bt26-03