CYBER ADVISORY

Wednesday, July 08, 2026 **CAL-CSIC-202607-A-003**

Multiple Vulnerabilities Impacting BeyondTrust's Remote Support and Privileged Remote Access

Access Control Bypass	Unauthorized Access	Denial-of-Service	Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of four vulnerabilities impacting BeyondTrust's Remote Support and Privileged Remote Access products. CVE-2026-40138 is an Improper Authentication vulnerability that carries a CVSS 4.0 score of 9.2.[1] CVE-2026-40139 is an Improper Authentication vulnerability that carries a CVSS 4.0 score of 9.2.[2] CVE-2026-40140 is an Uncontrolled Resource Consumption vulnerability that carries a CVSS 4.0 score of 8.7.[3] CVE-2026-40141 an Improper Neutralization of Special Elements in Data Query Logic vulnerability that carries a CVSS 4.0 score of 8.5.[4]

CVE-2026-40138 is a critical pre-authentication vulnerability that exists in the authentication subsystem of BeyondTrust's Remote Support and Privilege Remote access. Exploitation does require a specific authentication configuration to be enabled. Successful exploitation allows an attacker with network access to bypass access controls and gain unauthorized access to the target appliance, including accounts with elevated privileges.

CVE-2026-40139 is a second critical pre-authentication vulnerability that exists in the authentication subsystem of BeyondTrust's Remote Support. This vulnerability also requires a specific authentication configuration to be enabled. Successful authentication allows improper processing of authentication request that enables unauthenticated *remote* attackers to bypass access controls and gain unauthorized access to the target appliance, including accounts with elevated privileges.

CVE-2026-40140 is a high-severity pre-authentication vulnerability that exists in the network communication subsystem. This vulnerability is rooted in an insufficient validation of client-supplied input. Successful exploitation allows an unauthenticated *remote* attacker to trigger a denial-of-service (DoS) condition that impacts the availability of the targeted appliance.

CVE-2026-40141 is a high-severity vulnerability that exists in the web application component of BeyondTrust's Remote Support and Privileged Remote Access related to the processing of certain input parameters. This vulnerability is rooted in the insufficient validation of user-supplied input. Successful exploitation is restricted to accounts with specific permissions and allows an authenticated attacker with limited privileges to access unintended resources or data beyond their authorized scope.[5]

BeyondTrust internally identified and acknowledged these vulnerabilities and have issued a security advisory with a patch and mitigation instructions. There currently is no confirmed exploitation in the wild or as zero-day vulnerabilities.

The Cal-CSIC recommends following BeyondTrust's security advisory for patching and mitigation guidance as soon as possible. For additional details on these vulnerabilities, please use this link:

BeyondTrust Security Bulletin:

https://www.beyondtrust.com/trust-center/security-advisories/bt26-03

Affected Products and Versions

Product	Version
Remote Support (RS)	RS 25.3.2 or lower
Privileged Remote Access (PRA)	PRA 25.3.2 or lower

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] NVD; “CVE-2026-40138 Detail”; https://nvd.nist.gov/vuln/detail/CVE-2026-40138; accessed 8 July 2026
[2] NVD; “CVE-2026-40139 Detail”; https://nvd.nist.gov/vuln/detail/CVE-2026-40139; accessed 8 July 2026
[3] OpenCVE; CVE-2026-40140”; https://app.opencve.io/cve/CVE-2026-40140; accessed 8 July 2026
[4] OpenCVE; CVE-2026-40141”; https://app.opencve.io/cve/CVE-2026-40141; accessed 8 July 2026
[5] BeyondTrust; “BT26-03”; https://www.beyondtrust.com/trust-center/security-advisories/bt26-03; accessed 8 July 2026