

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



RCE Vulnerability in BeyondTrust Tools

Tracking #:432317393

Date:19-06-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity remote code execution (RCE) vulnerability has been identified in the chat functionality of BeyondTrust's Remote Support and Privileged Remote Access platforms.

TECHNICAL DETAILS:

A high-severity remote code execution (RCE) vulnerability, tracked as CVE-2025-5309, has been identified in the chat functionality of Remote Support and Privileged Remote Access platforms. This vulnerability stems from a Server-Side Template Injection (SSTI) flaw, allowing an unauthenticated attacker (in some cases) to inject and execute arbitrary code on the server.

Cloud-hosted customers have already been patched as of June 16, 2025. However, on-premise deployments remain at risk until the appropriate patches are applied. This vulnerability poses a significant threat to environments that expose affected versions of RS/PRA to the internet or untrusted users.

Vulnerability Details:

- Severity: High
- CVSSv4 Score: 8.6
- CVSS Vector: AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
- CVE ID: CVE-2025-5309
- CWE: CWE-94 – Improper Control of Generation of Code ('Code Injection')
- Affected Products: Remote Support (RS), Privileged Remote Access (PRA)
- Exploitation Status: No confirmed exploitation in the wild (as of advisory date)
- Affected Products:
 - Remote Support-24.2.2 – 24.2.4, 24.3.1 – 24.3.3, 25.1.1
 - Privileged Remote Access 24.2.2 – 24.2.4, 24.3.1 – 24.3.3, 25.1.1

Fixed version:

| Product | Version |
|--------------------------|--|
| Remote Support | 24.2.2 to 24.2.4 with HELP-10826-2 Patch |
| Remote Support | 24.3.1 to 24.3.3 with HELP-10826-2 Patch |
| Remote Support | 24.3.4 and any future 24.3.x release |
| Privileged Remote Access | 25.1.1 with HELP-10826-1 Patch |
| Privileged Remote Access | 25.1.2 and above |
| Privileged Remote Access | 24.2.2 to 24.2.4 with HELP-10826-2 Patch |
| Privileged Remote Access | 24.3.1 to 24.3.3 with HELP-10826-2 Patch |
| Privileged Remote Access | 25.1.1 with HELP-10826-1 Patch |

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to immediately update the affected versions to the fixed or latest versions released by BeyondTrust.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://www.beyondtrust.com/trust-center/security-advisories/bt25-04>