BeyondTrust Remote Support 6.0 Cross Site Scripting

2022.01.04

Credit: **Malcrove (https://cxsecurity.com/author/Malcrove/1/)**

Risk: **Low**

Local: **No**

Remote: **Yes**

CVE: **CVE-2021-31589 (https://cxsecurity.com/cveshow/CVE-2021-31589/)**

CWE: **CWE-79 (https://cxsecurity.com/cwe/CWE-79)**

Dork: (See Dorks List) intext:"BeyondTrust" "Redistribution Prohibited"

(https://cxsecurity.com/dorks/)

CVSS Base Score: **9.3/10**
Exploitability Subscore: **8.6/10**
Attack complexity: **Medium**
Confidentiality impact: **Complete**
Availability impact: **Complete**

Impact Subscore: **10/10**
Exploit range: **Remote**
Authentication: **No required**
Integrity impact: **Complete**

```
# Exploit Title: BeyondTrust Remote Support - Reflected Cross-Site Scripting (XSS)  (Unauthenticated)
# Google Dork: intext:"BeyondTrust" "Redistribution Prohibited"
# Date: 30/12/2021
# Exploit Author: Malcrove
# Vendor Homepage: https://www.beyondtrust.com/
# Version: v6.0 and earlier versions
# CVE: CVE-2021-31589

Summary:

Unauthenticated cross-site scripting (XSS) vulnerability in BeyondTrust Secure Remote Access Base Software through 6.0.1 allow remote attackers to inject arbitrary web script or HTML. Remote attackers could acheive full admin access to the appliance, by tricking the administrator into creating a new admin account through an XSS/CSRF attack involving a crafted request to the /appliance/users?action=edit endpoint.


Vulnerability Details:

Affected Endpoint: /appliance/login
Affected Parameter: login[password]
Request Method: GET or POST


Proof of concept (POC):

By navigating to the below link from a modern web browser, alert(document.domain) Javascript method would be fired in the same context of Beyondtrust Remote Support domain.

http://<bomgar-host>/appliance/login?login%5Bpassword%5D=test%22%3E%3Csvg/onload=alert(document.domain)%3E&login%5Buse_curr%5D=1&login%5Bsubmit%5D=Change%20Password


Mitigation:

A fix has been released by the vendor in NSBase 6.1. It's recommended to update the vulnerable appliance base version to the latest version.

- Time-Line:

    April 6, 2021: Vulnerability advisory sent to the vendor (Beyondtrust)
    April 8, 2021: Recevied an initial reply from the vendor
    Jun 10, 2021: The vendor released a fix for the vulnerability in NSbase 6.1
    Dec 30, 2021: The Responsible public disclosure
```

```
- Credits
Ahmed Aboul-Ela (Malcrove)
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2022010013)

T\ Lul

Vote for this issue: 👍 0 👎 -1

0% 100%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)