BeyondTrust Remote Support 6.0 Cross Site Scripting

Authored by Malcrove

Posted Jan 3, 2022

BeyondTrust Remote Support versions 6.0 and below suffer from a cross site scripting vulnerability.

tags | exploit, remote, xss
advisories | CVE-2021-31589
SHA-256 | c974011f5f45022352dcdbc5bd9c817581fc98bdbc3b7b45a41e107214bb693a Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# 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=Cl


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)
```

Login or Register to add favorites

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11secur1ty 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter

Subscribe to an RSS Feed