Securepoint SSL VPN Client 2.0.30 Local Privilege Escalation

Authored by Florian Bogner | Site bogner.sh

Posted Jun 30, 2021

Securepoint SSL VPN Client version 2.0.30 suffers from a local privilege escalation vulnerability.

tags | exploit, local
advisories | CVE-2021-35523
SHA-256 | 089fd391bbbeb7b8efda804fd0ad063d9c658488180ed9ca54ab3ba8f1db9424 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
Local Privilege Escalation in Securepoint SSL VPN Client 2.0.30

Metadata
====================================================
Release Date: 29-Jun-2021
Author: Florian Bogner @ https://bee-itsecurity.at
Affected product:  Securepoint SSL VPN Client
Fixed in: version 2.0.32
Tested on: Windows 10 x64 fully patched
CVE:  CVE-2021-35523
URL: https://bogner.sh/2021/06/local-privilege-escalation-in-securepoint-ssl-vpn-client-2-0-30/
Vulnerability Status: Fixed with new release

Vulnerability Description (copied from the CVE Details)
====================================================
Securepoint SSL VPN Client v2 before 2.0.32 on Windows has unsafe configuration handling that enables local
privilege escalation to NT AUTHORITY\SYSTEM. A non-privileged local user can modify the OpenVPN configuration
stored under "%APPDATA%\Securepoint SSL VPN" and add a external script file that is executed as privileged
user.

A full vulnerability description is available here: https://bogner.sh/2021/06/local-privilege-escalation-in-
securepoint-ssl-vpn-client-2-0-30/

Suggested Solution
====================================================
End-users should update to the latest available version.

Disclosure Timeline
====================================================
14.04.2021: The vulnerability was discovered and reported to security@securepoint.de
15.04.2021: The report was triaged
26.04.2021: Securepoint SSL VPN Client Version 2.0.32 was released, which contains an initial fix for the
vulnerability
23.06.2021: Securepoint SSL VPN Client Version 2.0.34 was released, which contains additional security
measures.
28.06.2021: CVE-2021-35523 was assigned: https://nvd.nist.gov/vuln/detail/CVE-2021-35523
29.06.2021: Responsible disclosure in cooperation with Securepoint: https://github.com/Securepoint/openvpn-
client/security/advisories/GHSA-v8p8-4w8f-qh34


___________

Florian Bogner
Information Security Expert, Speaker

Bee IT Security Consulting GmbH
Nibelungenstraße 37
3123 A-Schweinern

Mail: florian.bogner@bee-itsecurity.at
Web: https://www.bee-itsecurity.at
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

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