Investigating FortiManager Zero-Day Exploitation (CVE-2024-47575)

cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575/

Mandiant

Written by: Foti Castelan, Max Thauer, JP Glab, Gabby Roncone, Tufail Ahmed, Jared Wilson

Summary

In October 2024, Mandiant collaborated with Fortinet to investigate the mass exploitation of FortiManager appliances across 50+ potentially compromised FortiManager devices in various industries. The vulnerability, CVE-2024-47575 / FG-IR-24-423, allows a threat actor to use an unauthorized, threat actor-controlled FortiManager device to execute arbitrary code or commands against vulnerable FortiManager devices.

Mandiant observed a new threat cluster we now track as UNC5820 exploiting the FortiManager vulnerability as early as June 27, 2024. UNC5820 staged and exfiltrated the configuration data of the FortiGate devices managed by the exploited FortiManager. This data contains detailed configuration information of the managed appliances as well as the users and their FortiOS256-hashed passwords. This data could be used by UNC5820 to further compromise the FortiManager, move laterally to the managed Fortinet devices, and ultimately target the enterprise environment.

At this time, the data sources analyzed by Mandiant did not record the specific requests that the threat actor used to leverage the FortiManager vulnerability. Additionally, at this stage of our investigations there is no evidence that UNC5820 leveraged the obtained configuration data to move laterally and further compromise the environment. As a result, at the time of publishing, we lack sufficient data to assess actor motivation or location. As additional information becomes available through our investigations, Mandiant will update this blog's attribution assessment.

Organizations that may have their FortiManager exposed to the internet should conduct a forensic investigation immediately.

Exploitation Details

Mandiant's earliest observed exploitation attempt occurred on June 27, 2024. On that day, multiple FortiManager devices received inbound connections from the IP address 45[.]32[.]41[.]202 on the default port TCP/541. At approximately the same time, the file

system recorded the staging of various Fortinet configuration files in a Gzip-compressed archive named /tmp/.tm. This archive contained the files and folders as listed in Table 1.

Filename	Description
/var/dm/RCS	Folder containing configuration files of managed FortiGate devices
/var/dm/RCS/revinfo.db	Database containing additional information of the managed FortiGate devices
/var/fds/data/devices.txt	Contains a list of FortiGate serials and their corresponding IP addresses
/var/pm2/global.db	Global database that contains object configurations, policy packages, and header and footer sensor configuration for IPS
/var/old_fmversion	Contains current FortiManager version, build, and branch information

Table 1: Content of /tmp/.tm

On Sept. 23, 2024, Mandiant observed a second exploitation attempt with the same indicators. In both exploitation events, outbound network traffic occurred shortly after the archive creation. The amount of bytes sent to the respective destination IP addresses are slightly larger than the size of the archive. Table 2 lists the details of this activity.

Timestamp	Description	Size
2024-06-27 12:44:04	/tmp/.tm (File creation)	Unknown
2024-06-27 12:44:11	Outbound traffic to 195[.]85[.]114[.]78:443	1,819,425 bytes
2024-09-23 11:31:12	/tmp/.tm (File modification)	1,772,650 bytes
2024-09-23 11:31:19	Outbound traffic to 104[.]238[.]141[.]143:443	1,822,968 bytes

Table 2: Correlation of staged configuration data and outbound traffic of the two exploitation attempts

During the second exploitation attempt, the threat actor's device was registered to the targeted FortiManager. Figure 1 lists the unauthorized FortiManager in the Global Objects database along with the timestamp when it was added.

```
SELECT oid, name, sn, platform_str, ip, mgmt_if, datetime(last_checked, 'unixepoch') as last_checked, datetime(first_tunnel_up, 'unixepoch') as first_tunnel_up
FROM device
where name = 'localhost'
```

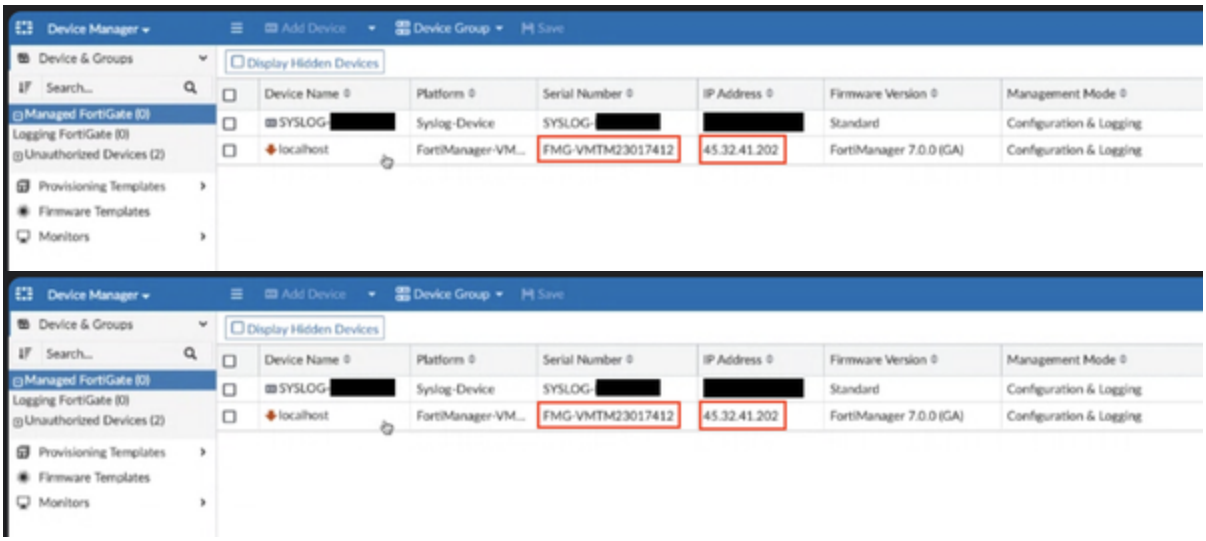
	oid	name	sn	platform_str	ip	mgmt_if	last_checked	first_tunnel_up
1	1932	localhost	FMG-VMTM23017412	FortiManager-VM64	45.32.41.202	port1	2024-09-22 10:01:49	2024-09-22 10:01:43


```
SELECT oid, name, sn, platform_str, ip, mgmt_if, datetime(last_checked, 'unixepoch') as last_checked, datetime(first_tunnel_up, 'unixepoch') as first_tunnel_up
FROM device
where name = 'localhost'
```

	oid	name	sn	platform_str	ip	mgmt_if	last_checked	first_tunnel_up
1	1932	localhost	FMG-VMTM23017412	FortiManager-VM64	45.32.41.202	port1	2024-09-22 10:01:49	2024-09-22 10:01:43

Figure 1: Threat actor's device added to Global Objects database

Once the threat actor successfully exploited the FortiManager, their unknown Fortinet device appeared in the FortiManager console.



Device Manager
Add Device
Device Group
Save
Device & Groups
Search...
Managed FortiGate (0)
Logging FortiGate (0)
Unauthorized Devices (2)
Provisioning Templates
Firmware Templates
Monitors
Display Hidden Devices
Device Name
Platform
Serial Number
IP Address
Firmware Version
Management Mode
SYSLOG-[redacted]
Syslog-Device
SYSLOG-[redacted]
[redacted]
Standard
Configuration & Logging
localhost
FortiManager-VM...
FMG-VMTM23017412
45.32.41.202
FortiManager 7.0.0 (GA)
Configuration & Logging

Figure 2: Unauthorized device listed in FortiManager console

An additional indicator of successful exploitation is the addition of the unauthorized device serial number "FMG-VMTM23017412" and its corresponding IP address 45[.]32[.]41[.]202 to the file /fds/data/unreg_devices.txt. Figure 3 lists the content of this file.

```
FMG-VMTM23017412|45.32.41.202
```

Figure 3: Content of /fds/data/unreg_devices.txt

The files /fds/data/subs.dat and /fds/data/subs.dat.tmp contain additional indicators of the exploitation that include an associated disposable email address and a company name as listed in Figure 4.

```
SerialNumber=FMG-VMTM23017412|AccountID=
0qsc137p@justdefinition.com|Company=Purity Supreme|UserID=1756868
```

Figure 4: Content of /fds/data/subs.dat

Mandiant scraped the FortiManager's memory image for additional artifacts of threat actor activity and detected a JSON blob containing the keywords "FMG-VMTM23017412" and "45[.]32[.]41[.]202". This JSON blob also included a "first_tunnel_up" key, which contained the epoch time of 1726999303 as its value. This timestamp translates to 2024-09-22 10:01:43 UTC.

```
fex_cnt: 0
first_tunnel_up: 1726999303
flags: 257
foslic_cpu: 0
foslic_dr_site: 0
foslic_inst_time: 0
foslic_last_sync: 0
foslic_ram: 0
foslic_type: 0
foslic_utm: 0
fsw_cnt: 0
ha_group_id: 0
ha_group_name: ""
ha_mode: 0
ha_slave: null
hdisk_size: 30720
hostname: "localhost"
hw_generation: 0
hw_rev_major: 0
hw_rev_minor: 0
hyperscale: 0
ip: "45.32.41.202"
ips_ext: 0
ips_ver: ""
```

```
mr: 0
name: "localhost"
node_flags: 0
nsxt_service_name: ""
oid: 1932
onboard_rule: null
opts: 0
os_type: 9
os_ver: 7
patch: 0
platform_str: "FortiManager-VM64"
prefer_img_ver: ""
prio: 0
private_key: ""
private_key_status: 0
psk: ""
role: 0
sn: "FMG-VMTM23017412"
source: 1
```



```
fex_cnt: 0
first_tunnel_up: 1726999303
flags: 257
foslic_cpu: 0
foslic_dr_site: 0
foslic_inst_time: 0
foslic_last_sync: 0
foslic_ram: 0
foslic_type: 0
foslic_utm: 0
fsw_cnt: 0
ha_group_id: 0
ha_group_name: ""
ha_mode: 0
ha_slave: null
hdisk_size: 30720
hostname: "localhost"
hw_generation: 0
hw_rev_major: 0
hw_rev_minor: 0
hyperscale: 0
ip: "45.32.41.202"
ips_ext: 0
ips_ver: ""
```

```
mr: 0
name: "localhost"
node_flags: 0
nsxt_service_name: ""
oid: 1932
onboard_rule: null
opts: 0
os_type: 9
os_ver: 7
patch: 0
platform_str: "FortiManager-VM64"
prefer_img_ver: ""
prio: 0
private_key: ""
private_key_status: 0
psk: ""
role: 0
sn: "FMG-VMTM23017412"
source: 1
```

Figure 5: Tunnel up artifacts

Lack of Follow-On Malicious Activity

Mandiant reviewed the rootfs.gz, which is an initramfs (RAM disk) for the device that gets mounted to /bin. We did not find any malicious files created or modified during the time frame of exploitation activity.

Google Cloud notified affected customers who showed similar activity in their environments. Additionally, Google Threat Intelligence ran retrohunts while developing detections for this activity, and manually escalated Pre-Release Detection Rule alerts to affected SecOps customers to assist with detecting exploit attempts of Fortinet devices.

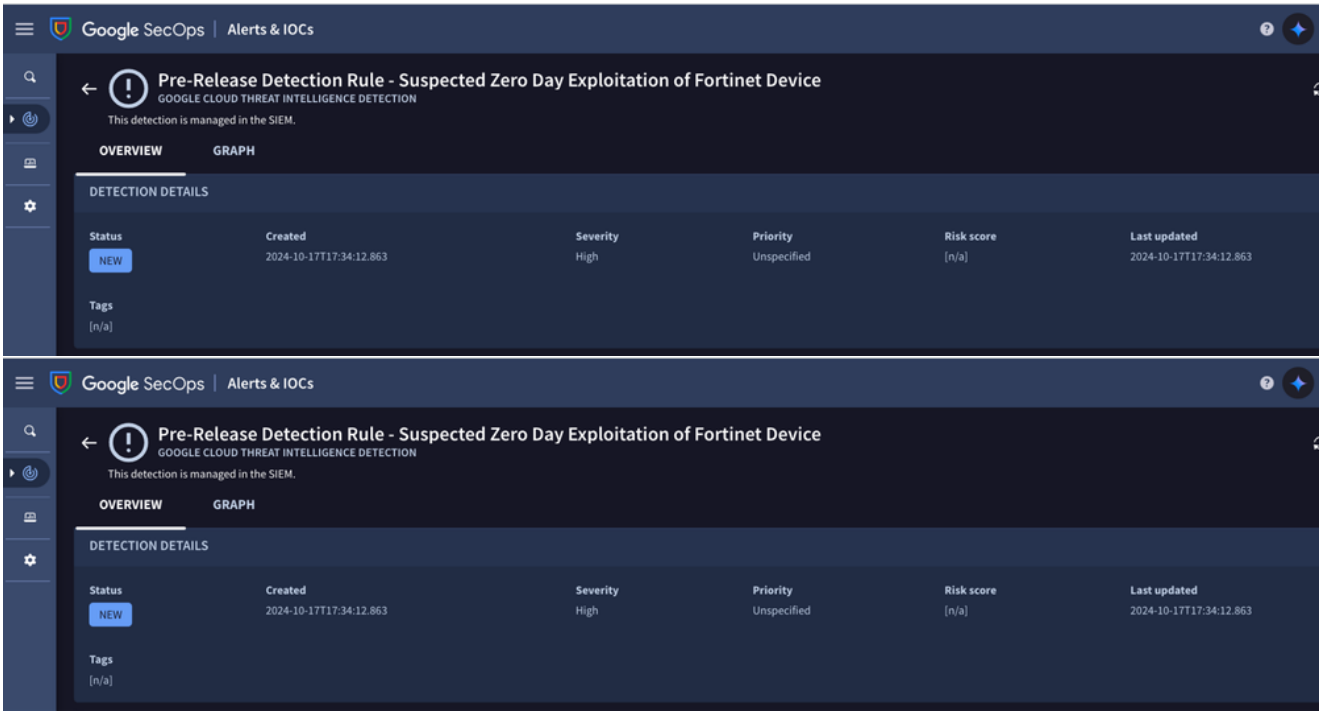


Figure 6: Pre-Release Detection Rule — Suspected Zero Day Exploitation of Fortinet Device

In addition to collaborating with Mandiant, Fortinet proactively sent advance communications to its customers as an early warning on their advisory to enable customers to strengthen their security posture prior to broad public disclosure.

Timeline of Threat Actor Activity

Timestamp	Event
2024-06-27 12:44:04	Inbound network connection from 45[.]32[.]41[.]202.File creation: /tmp/.tm

2024-06-27 12:44:07	Outbound network connection to 45[.]32[.]41[.]202 on port 443
2024-06-27 12:44:11	Outbound network connection to 195[.]85[.]114[.]78 on port 443. The bytes sent are approximately equal to the size of /tmp/.tm
2024-09-22 10:01:47	Inbound network connection from 45[.]32[.]41[.]202
2024-09-22 10:01:50	Outbound network connections to 158[.]247[.]199[.]37:443 and 45[.]32[.]41[.]202:443. The connections to 158[.]247[.]199[.]37 were denied
2024-09-22 10:02:21	String indicating exploitation in /log/locallog/elogmsg="Unregistered device localhost add succeeded"
2024-09-22 10:02:55	File modified: /fds/data/unreg_devices.txtContents: “FMG-VMTM23017412|45.32.41.202”
2024-09-22 10:07:36	String indicating exploitation in /log/locallog/elogchanges="Edited device settings (SN FMG-VMTM23017412)"
2024-09-23 11:31:12	Inbound network connection to destination port 541 from 45[.]32[.]41[.]202File modified: /tmp/.tm
2024-09-23 11:31:16	Outbound network connection to 104[.]238[.]141[.]143. The bytes sent are approximately equal to the size of /tmp/.tm

Table 3: Timeline of activity

Mitigation Strategies / Workaround

1. Limit access to FortiManager admin portal for only approved internal IP addresses.
2. Only allow permitted FortiGate addresses to communicate with FortiManager.
3. Deny unknown FortiGate devices from being associated with FortiManager.

Available 7.2.5, 7.0.12, 7.4.3 and later (not functional workaround on 7.6.0).

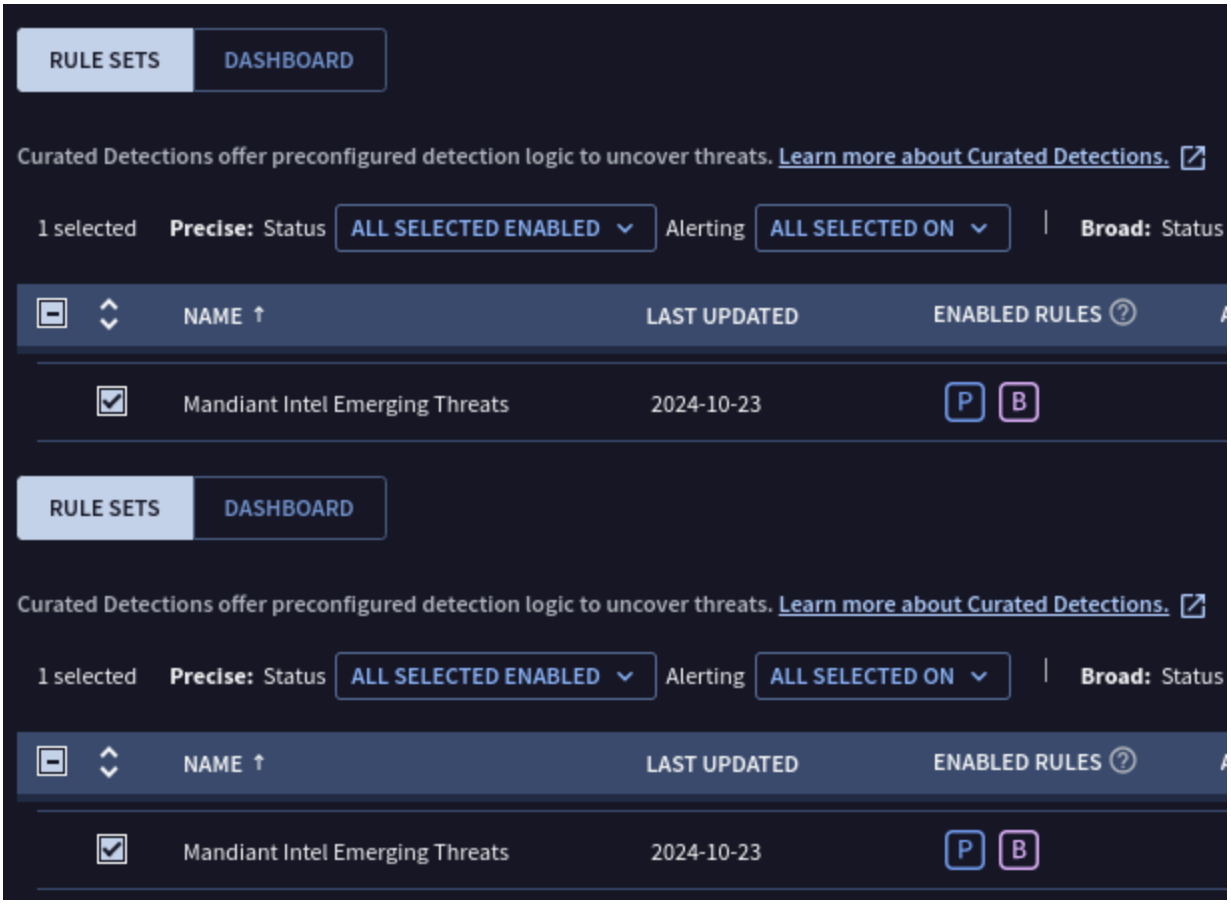
```
config system global
    set fgfm-deny-unknown enable
end
```

Figure 7: Configuration to deny unknown devices

Detection

YARA-L

If you are a Google SecOps Enterprise+ customer, rules were released to the "Mandiant Intel Emerging Threats" rule pack (within the Windows Threats group).



Relevant Rules

- `Suspicious FortiManager Inbound and Outbound Connection`
- `UNC5820 Fortinet Exploitation and File Download`
- `UNC5820 Fortinet Exploitation and non-HTTPS Command and Control`
- `UNC5820 Fortinet Exploitation and HTTPS Command and Control`

Other SIEMs

Develop searches against Fortiguard logs for the following relevant IOCs. In particular, the Malicious Fortinet Device ID should provide a high fidelity alert if triggered.

Baseline and set thresholds for unique operations in the FortiManager logs. In particular, operations for “Add device” and “Modify device” may be rare enough for your organization to provide an actionable alert until this vulnerability can be patched.

Similarly, baseline and set thresholds for the changes field in the FortiManager logs, and consider a higher sensitivity when the changes field includes the word ‘Unregistered’.

Enumerate the Fortigate devices daily, and alert when a previously unseen device name is observed in the logs.

Indicators of Compromise (IOCs)

A Google Threat Intelligence Collection of IOCs is available for registered users.

Network-Based IOCs

IOC	Description
45.32.41.202	UNC5820
104.238.141.143	UNC5820
158.247.199.37	UNC5820
195.85.114.78	UNC5820

Host-Based IOCs

IOC	Description
.tm	Archive of config files
9DCFAB171580B52DEAE8703157012674	MD5 hash of unreg_devices.txt

Additional Keywords

Keyword	Description

FMG-VMTM23017412	Malicious Fortinet Device ID
msg="Unregistered device localhost add succeeded"	String indicating exploitation in /log/locallog/elog
changes="Edited device settings (SN FMG-VMTM23017412)"	String indicating exploitation in /log/locallog/elog
changes="Added unregistered device to unregistered table."	String indicating exploitation in /log/locallog/elog
0qsc137p@justdefinition.com	Observed in subs.dat and subs.dat.tmp. This is a disposable email address created by the threat actor.
Purity Supreme	Observed in subs.dat and subs.dat.tmp

Acknowledgements

We would like to thank Nick Simonian and Ronnie Salomonsen for their contributions.

Webinar

Two authors of this blog post, Foti Castelan and Max Thauer, will be presenting additional details and mitigation strategies during a Nov. 6 webinar. Register now to learn more about this threat, and how to defend against it.

Posted in

Threat Intelligence