CERT-EU

**Security Advisory 2024-113**

# Critical 0-day Vulnerability in Fortinet FortiManager

***2024-10-24 — v1.1***

**TLP:CLEAR**

*History:*

- *23/10/2024 — v1.0 – Initial publication*
- *24/10/2024 — v1.1 – Fix incorrect CVE identifier*

## Summary

On October 23, 2024, Fortinet released a security advisory addressing a critical 0-day vulnerability in its FortiManager product. If exploited, a remote unauthenticated attacker could execute arbitrary code or commands on the affected device [1].

It is strongly recommended applying the update. When not possible, it is recommended applying the workaround. In all cases, it is recommended searching for potential compromise.

## Technical Details

The vulnerability **CVE-2024-47575**, with a CVSS score of 9.8, affects FortiManager fgfmd daemon, and is due to a missing authentication for critical function. A remote unauthenticated attacker could execute arbitrary code or commands via specially crafted requests.

## Affected Products

The following product versions are affected:

- FortiManager 7.6 versions before 7.6.1;
- FortiManager 7.4 versions before 7.4.5;
- FortiManager 7.2 versions before 7.2.8;
- FortiManager 7.0 versions before 7.0.13;
- FortiManager 6.4 versions before 6.4.15;
- FortiManager 6.2 versions before 6.2.13;
- FortiManager Cloud 7.4 versions before 7.4.5;
- FortiManager Cloud 7.2 all versions;
- FortiManager Cloud 7.0 all versions;
- FortiManager Cloud 6.4 all versions;

## Recommendations

It is strongly recommended updating affected devices as soon as possible, prioritising Internet facing assets. When not possible, it is strongly recommended applying the workaround.

It is also strongly encouraged looking for potential compromise.

### Workaround

1. For FortiManager versions 7.0.12 or above, 7.2.5 or above, 7.4.3 or above (but not 7.6.0), prevent unknown devices from attempting to register:

```
config system global
(global)# set fgfm-deny-unknown enable
(global)# end
```

*Warning: With this setting enabled, be aware that if a FortiGate's SN is not in the device list, FortiManager will prevent it from connecting to register upon being deployed, even when a model device with PSK is matching.*

2. For FortiManager versions 7.2.0 and above, one may add local-in policies to whitelist the IP addresses of FortiGates that are allowed to connect.

Example:

```
config system local-in-policy
edit 1
set action accept
set dport 541
set src
next
edit 2
set dport 541
next
end
```

3. For 7.2.2 and above, 7.4.0 and above, 7.6.0 and above it is also possible to use a custom certificate which will mitigate the issue:

```
config system global
set fgfm-ca-cert
set fgfm-cert-exclusive enable


end
```

And install that certificate on FortiGates. Only this CA will be valid, this can act as a workaround, providing the attacker cannot obtain a certificate signed by this CA via an alternate channel.

*NB: For FortiManager versions 6.2, 6.4, and 7.0.11 and below, upgrade to one of the versions above and apply the above workarounds.*

### IoC Detections

The following indicators of compromise could be used to identify potential compromise. Note that file IoCs may not appear in all cases.

### Logs

```
type=event,subtype=dvm,pri=information,desc="Device,manager,generic,information,log",user="devi
  ce,...",msg="Unregistered device localhost add succeeded" device="localhost"
  adom="FortiManager" session_id=0 operation="Add device" performed_on="localhost"
  changes="Unregistered device localhost add succeeded"


type=event,subtype=dvm,pri=notice,desc="Device,Manager,dvm,log,at,notice,level",user="System",u
  serfrom="",msg="" adom="root" session_id=0 operation="Modify device" performed_on="localhost"
   changes="Edited device settings (SN FMG-VMTM23017412)"
```

### IP addresses

```
45.32.41.202
104.238.141.143
158.247.199.37
45.32.63.2
```

### Serial Number

`FMG-VMTM23017412`

### Files

```
/tmp/.tm
/var/tmp/.tm
```

## References

[1] https://www.fortiguard.com/psirt/FG-IR-24-423