مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Fortinet FortiManager Critical Zero Day Vulnerability

Tracking #:432316433-Update
Date:31-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Fortinet's FortiManager API has been disclosed and is actively exploited in the wild.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2024-47575) in Fortinet's FortiManager API has been disclosed and is actively exploited in the wild. This flaw allows unauthenticated remote attackers to execute arbitrary code or commands, potentially leading to data theft and network compromise. The vulnerability affects multiple versions of FortiManager, including both on-premises and cloud deployments.

Key points:

- **CVE-2024-47575** has a CVSS score of 9.8 out of 10
- Attackers have exploited this flaw to steal sensitive data, including device configurations, IP addresses, and credentials
- The vulnerability impacts FortiManager versions 6.2.x through 7.6.0
- Fortinet has released patches for some affected versions and provided mitigation strategies

Vulnerability Details:

- CVE-2024-47575 is an authentication bypass vulnerability in the FortiManager fgfmd daemon. It allows unauthenticated attackers to execute arbitrary code or commands through specially crafted requests.
- Attackers must first obtain a valid certificate from a compromised or owned Fortinet device. They can then connect to exposed FortiManager servers and exploit the vulnerability in the FGFM API to bypass authentication and execute commands.

Version	Affected	Solution
FortiManager 7.6	7.6.0	Upgrade to 7.6.1 or above
FortiManager 7.4	7.4.0 through 7.4.4	Upgrade to 7.4.5 or above
FortiManager 7.2	7.2.0 through 7.2.7	Upgrade to 7.2.8 or above
FortiManager 7.0	7.0.0 through 7.0.12	Upgrade to 7.0.13 or above
FortiManager 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above
FortiManager 6.2	6.2.0 through 6.2.12	Upgrade to 6.2.13 or above
FortiManager Cloud 7.6	Not affected	Not Applicable
FortiManager Cloud 7.4	7.4.1 through 7.4.4	Upgrade to 7.4.5 or above
FortiManager Cloud 7.2	7.2.1 through 7.2.7	Upgrade to 7.2.8 or above
FortiManager Cloud 7.0	7.0.1 through 7.0.12	Upgrade to 7.0.13 or above
FortiManager Cloud 6.4	6.4 all versions	Migrate to a fixed release

Observed Attacks:

- Threat actors have stolen files containing configurations, IP addresses, and credentials of managed devices
- Attackers used rogue FortiGate devices with the name "localhost" and serial number FMG-VMTM23017412
- Several IP addresses associated with the Vultr cloud hosting company were observed in the attacks

Monitor for the following Indicators of Compromise:

- Unregistered devices named "localhost" in FortiManager
- Log entries showing API commands to add unregistered "localhost" devices
- Presence of /tmp/.tm and /var/tmp/.tm files
- Connections from the following IP addresses:
  - 45.32.41.202
  - 104.238.141.143
  - 158.247.199.37
  - 45.32.63.2

Update: New IOCs:

- 80.66.196.199
- 104.238.141.143
- 158.247.199.37
- 195.85.114.78
- 172.232.167.68

Serial Number:

- FMG-VMTM19008093

RECOMMENDATIONS:

- Update Immediately: Upgrade to the latest patched version of FortiManager as soon as possible.
- Apply Mitigations: If immediate patching is not feasible, implement the recommended mitigations.
- Monitor for Indicators of Compromise: Check for unauthorized "localhost" devices in the Unregistered Devices section and review logs for suspicious API commands.
- Enhance Network Segmentation: Isolate FortiManager instances from direct internet access where possible.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://fortiguard.fortinet.com/psirt/FG-IR-24-423