Forensic Technology Solutions

Threat Alert: 1/10/2024: FortiGate, FortiManager zero-day exploitation

29 October 2024

pwc

Background

We have prepared this document based on research conducted on the risks and vulnerabilities associated with Fortinet's FortiManager software. In this publication, our focus is on a vulnerability, disclosed in October 2024, that allows an attacker to remotely gain access and administer the FortiGate firewall devices that have been registered on the vulnerable FortiManager portal.

The output of our research is provided to you at no cost and is aimed at providing a value-added service as to how the potential losses of data can be limited by heightened awareness on the part of your business.

Introduction – Vulnerability discovery

Vulnerability discovery

Fortinet is a manufacturer of network security hardware and software. Common among these are firewalls, switches and network access control devices. For ease of administration Fortinet created FortiManager, a management portal for multiple Fortinet products across diverse networked environments.

A critical vulnerability has been discovered on multiple versions of FortiManager[1]. The vulnerability allows an attacker to remotely execute malicious code and issue arbitrary commands to Fortinet devices that have been registered on the affected version of FortiManager. As of 24 October 2024, Threat Intelligence reports that these flaws have been actively exploited in the wild from at least June 2024 on multiple occasions[2].

Exposure

From early October 2024, various posts on social media have been informing the public about this vulnerability, with Fortinet publishing a statement and advisory on 24 October 2024, allocating CVE-2024-47575[3] to the vulnerability. Between 13 and 23 October, security researchers conducting open-source intelligence searches determined that at least 60,000 internet accessible instances of the FortiManager portal were vulnerable to this flaw[4]. In addition to this, another critical vulnerability affecting FortiGate firewalls CVE-2024–23113 was reported. As of 15 October 2024, over 87,000 internet connected firewalls were still vulnerable to this flaw[5].

PwC conducted searches on publicly available social media posts for chatter about the vulnerability. We noted a spike in individuals speaking of 'FortiGate' and 'Zero Day' for the period spanning from 18 October to 24 October 2024.

This indicated that publicity around the issue is increasing and there is a possibility of more widespread exploitation in future. The adjacent screenshot shows the spike in interest on this issue together with the sentiment attached to the social media posts.

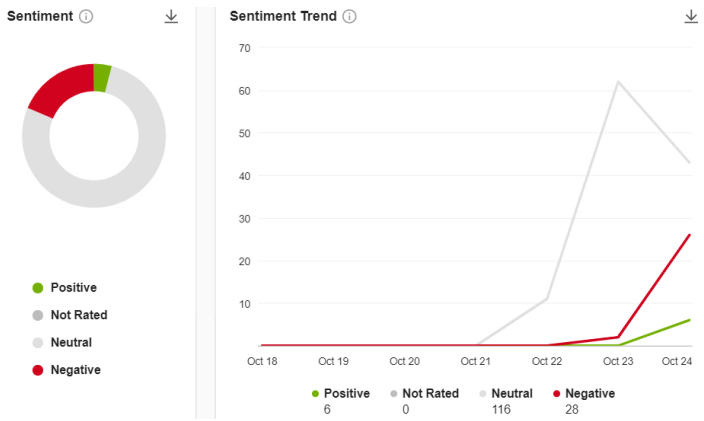

Figure 1 - Spike in interest on FortiGate

[1] https://securityaffairs.com/170175/hacking/us-cisa-adds-fortinet-fortimanager-flaw-known-exploited-vulnerabilities-catalog.html
[2] https://securityaffairs.com/170189/hacking/fortijump-flaw-exploited-since-june-2024.html
[3] https://fortiguard.fortinet.com/psirt/FG-IR-24-423
[4] https://doublepulsar.com/burning-zero-days-fortijump-fortimanager-vulnerability-used-by-nation-state-in-espionage-via-msps-c79abec59773
[5] https://www.helpnetsecurity.com/2024/10/15/cve-2024-23113/

What is the risk to your organisation?

- **Unauthorised access:** Attackers may exploit the vulnerability to gain unauthorised access to the FortiManager portal to execute arbitrary commands.
- **Configuration changes:** With this level of access, attackers could alter or delete configurations and access control lists that are put in place on your perimeter security devices such as firewalls.
- **Network disruption:** Exploiting this vulnerability could lead to service disruptions, potentially affecting business operations
- **Wider network compromise**: Since FortiManager is often used to manage multiple Fortinet devices, an exploit could provide attackers to gain full access to a business's environment in the form of a full-scale cybersecurity breach.

What can you do?

Fortine has released an advisory detailing some of the recommended remediation actions that can immediately be applied to mitigate the risk introduced by this vulnerability[6]. At a high level, the following outlines some of these actions:

- Upgrade your version of FortiManager to the latest version.
- Limit access to FortiManager for the IP addresses that are included in the IOC list.
- Install a fresh FortiManager Virtual Machine or re-initialise a hardware model and re-add/discover managed devices in situations where the vulnerability has already been exploited.

Conclusion

The critical vulnerabilities in FortiManager pose significant risks to organisations using Fortinet products with the potential for unauthorised access, remote code execution and broader network compromises. Given the recent trends noted, the time delay between vulnerabilities being noted and exploitation has significantly decreased. As such, organisations should consider timely remediation to avoid being affected.

Appendix 1 – Indicators of Compromise (IOCs)

In October 2024 Mandiant collaborated with Fortinet to investigate the mass exploitation of FortiManager appliances. Listed below is a set of IOCs that were a result of their joint forensic investigation. Consider checking your environment for the following IOCs as a means to assess whether this vulnerability has been exploited in your environment[7]:

Log entries

type=event,subtype=dvm,pri=information,desc="Device,manager,generic,information,log",user="device,...",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",userfrom="",msg="" adom="root" session_id=0 operation="Modify device" performed_on="localhost" changes="Edited device settings (SN FMG-VMTM23017412)"

[6] https://fortiguard.fortinet.com/psirt/FG-IR-24-423
[7] https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575

IP addresses

45.32.41[.]202
104.238.141[.]143
158.247.199[.]37
45.32.63[.]2

Files and file paths

/tmp/.tm
/var/tmp/.tm
/var/dm/RCS
/var/dm/RCS/revinfo.db
/var/fds/data/devices.txt
/var/pm2/global.db
/var/old_fmversion

How Can PwC Help?

To have a deeper discussion about how to protect against or investigate digital compromises, please contact the PwC Forensic Technology Solutions team:

Junaid Amra
+27 (0) 82 953 9325
junaid.amra@pwc.com

Solomon Bhala
+27 (0) 65 970 6189
solomon.bhala.za@pwc.com