Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

UNC5820 Exploits Critical FortiManager Zero-Day to Hijack Enterprise Networks

Date of Publication	Admiralty Code	TA Number
October 24, 2024	A1	TA2024409

Summary

First Seen: June 27, 2024
Affected Products: Fortinet FortiManager
Actor: UNC5820
Impact: Fortinet has identified a zero-day vulnerability in the FortiManager API, tracked as CVE-2024-47575, which has been actively exploited in attacks. This flaw has resulted in the mass exploitation of over 50 potentially compromised FortiManager devices across various industries. Attackers have leveraged this vulnerability to steal sensitive files, including device configurations, IP addresses, and credentials. A new threat actor group, UNC5820, has been exploiting this vulnerability to stage and exfiltrate configuration data from FortiGate devices managed through the compromised FortiManager platform.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-47575	Fortinet FortiManager Missing Authentication Vulnerability	Fortinet FortiManager	✓	✓	✓

Vulnerability Details

#1

A critical vulnerability, identified as CVE-2024-47575, has been discovered in FortiManager, Fortinet’s centralized management platform for FortiGate devices. This flaw has led to the mass exploitation of over 50 potentially compromised FortiManager devices across various industries. The flaw allows remote, unauthenticated attackers to execute arbitrary code or commands by sending specially crafted requests. If successfully exploited, attackers can gain unauthorized access to sensitive configuration files, credentials, and device information, leading to potential system compromise. FortiManager is widely used in enterprise environments, making the exploitation of this vulnerability a significant risk for organizations that rely on its secure management of Fortinet devices.

#2 UNC5820 has been actively exploiting this vulnerability, first targeting a FortiManager system on June 27, 2024. During the attack, the malicious actors gained access to FortiGate devices managed by the compromised FortiManager, exfiltrating sensitive data such as configuration files, user credentials, and FortiOS256-hashed passwords. The attackers accessed TCP port 541, which is the default port for management traffic between FortiGate and FortiManager systems and staged the stolen files into a Gzip archive.

#3 Notably, UNC5820 also registered an unauthorized device to the FortiManager console, adding its serial number to the system. A second exploitation attempt occurred on September 23, 2024, with similar indicators, including outbound traffic shortly after file staging and the use of disposable email addresses linked to fake company identities.

#4 The attack demonstrated a high level of sophistication, as UNC5820 successfully registered their device on the compromised FortiManager system. The presence of this serial number, along with suspicious modifications to system files provided clear evidence of tampering. Additionally, the attackers used a disposable email and a fake company name, further obscuring their identity while maintaining persistent access to the system.

#5 Additionally, older FortiGate devices are vulnerable under specific conditions. The exploitation of CVE-2024-47575 by UNC5820 underscores the critical need for organizations to address vulnerabilities in their FortiManager systems immediately. By compromising FortiManager, attackers can gain control over an organization's security infrastructure, leading to widespread data exfiltration and potential future attacks on managed devices.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-47575	FortiManager 7.6.0, FortiManager 7.4.0 through 7.4.4, FortiManager 7.2.0 through 7.2.7, FortiManager 7.0.0 through 7.0.12, FortiManager 6.4.0 through 6.4.14, FortiManager 6.2.0 through 6.2.12, FortiManager Cloud 7.4.1 through 7.4.4, FortiManager Cloud 7.2.1 through 7.2.7, FortiManager Cloud 7.0.1 through 7.0.12, FortiManager Cloud 6.4 (all versions)	cpe:2.3:o:fortinet:fortimanager:*:*:*:*:*:*:*:*	CWE-306

Recommendations

Update: Users should immediately apply the latest patches for FortiManager or migrate to a secure release if utilizing FortiManager Cloud to protect against potential exploitation of CVE-2024-47575.

IP Whitelisting: Create an allowed list of IP addresses for FortiManager versions 7.2.0 and above devices that are permitted to connect to the FortiManager system. To enhance security, implement local-in policies that whitelist these IP addresses, ensuring that only authorized FortiGate devices can establish connections. This will significantly reduce the risk of unauthorized access or exploitation attempts.

Prevent Unknown Device: Enable the command set fgfm-deny-unknown enable to block devices with unknown serial numbers from registering to the FortiManager versions 7.0.12 or above, 7.2.5 or above, 7.4.3 or above (but not 7.6.0). This will ensure that only authorized devices with valid serial numbers can connect, adding an additional layer of protection against unauthorized access or potential exploitation.

Generate Custom Certificate: Generate and implement a custom SSL certificate to authenticate FortiGate devices with FortiManager for versions 7.2.2 and above, 7.4.0 and above, 7.6.0 and above, providing an additional security layer. This ensures that only devices with the valid CA can establish SSL tunnels, mitigating the risk of unauthorized access.

Device Recovery: Implement a robust backup strategy that includes regular backups of device configurations and critical data. Develop clear recovery procedures outlining steps to restore devices after a breach or failure and test these procedures regularly for effectiveness. Maintain documentation of recovery processes to streamline future efforts and ensure staff are trained on these protocols.

Monitor Device Logs and Change Passwords: Continuously monitor device logs for unusual activity, especially unauthorized login attempts or API requests. If any suspicious behavior is detected, immediately change administrative passwords and other critical credentials. Ensure that all passwords are strong, unique, and regularly updated. Implement multi-factor authentication (MFA) wherever possible to enhance security.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1036 Masquerading	T1016 System Network Configuration Discovery
T1587 Develop Capabilities	T1587.003 Digital Certificates	T1074 Data Staged	T1585 Establish Accounts
T1585.002 Email Accounts	T1059 Command and Scripting Interpreter	T1222 File and Directory Permissions Modification	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	45[.]32[.]41[.]202, 104[.]238[.]141[.]143, 158[.]247[.]199[.]37, 45[.]32[.]63[.]2, 195[.]85[.]114[.]78
Files	/tmp/.tm, /var/tmp/.tm
MD5	9DCFAB171580B52DEAE8703157012674
Serial Number	FMG-VMTM23017412
Email Address	0qsc137p@justdefinition[.]com

Patch Details

Fortinet has released fixed versions to address the vulnerability CVE-2024-47575. Users are encouraged to upgrade to these patched versions to mitigate the associated risks.

Upgrade to the following versions of FortiManager & FortiManager Cloud:
7.6.1 or higher
7.4.5 or higher
7.2.8 or higher
7.0.13 or higher
6.4.15 or higher
6.2.13 or higher

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

References

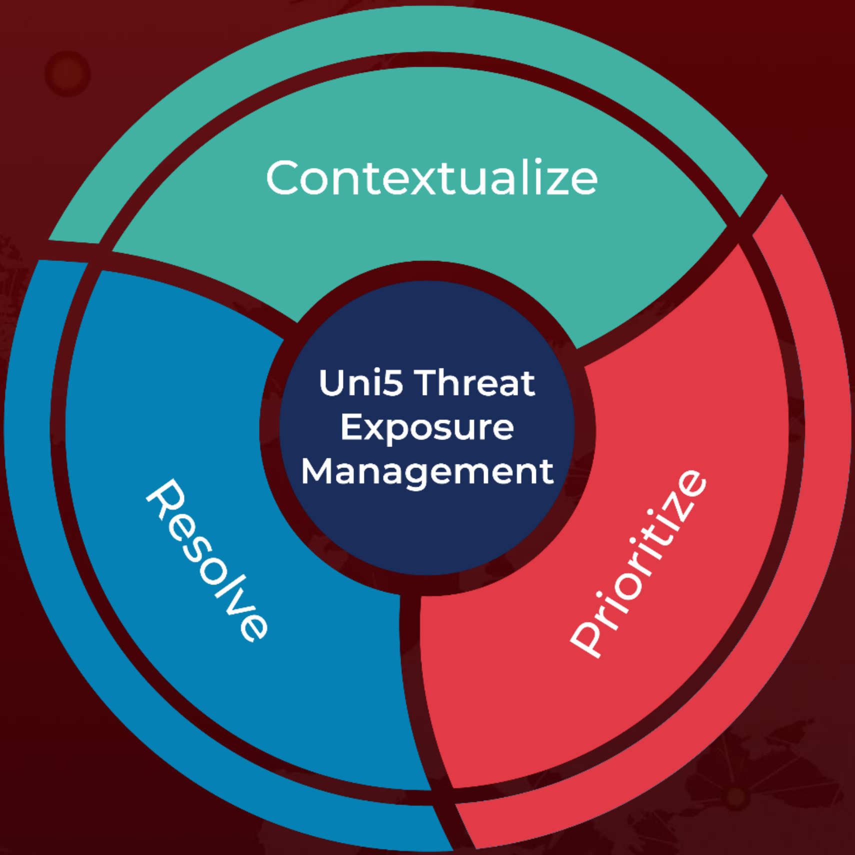
https://www.fortiguard.com/psirt/FG-IR-24-423

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

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 24, 2024 • 7:20 PM

More at www.hivepro.com