Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

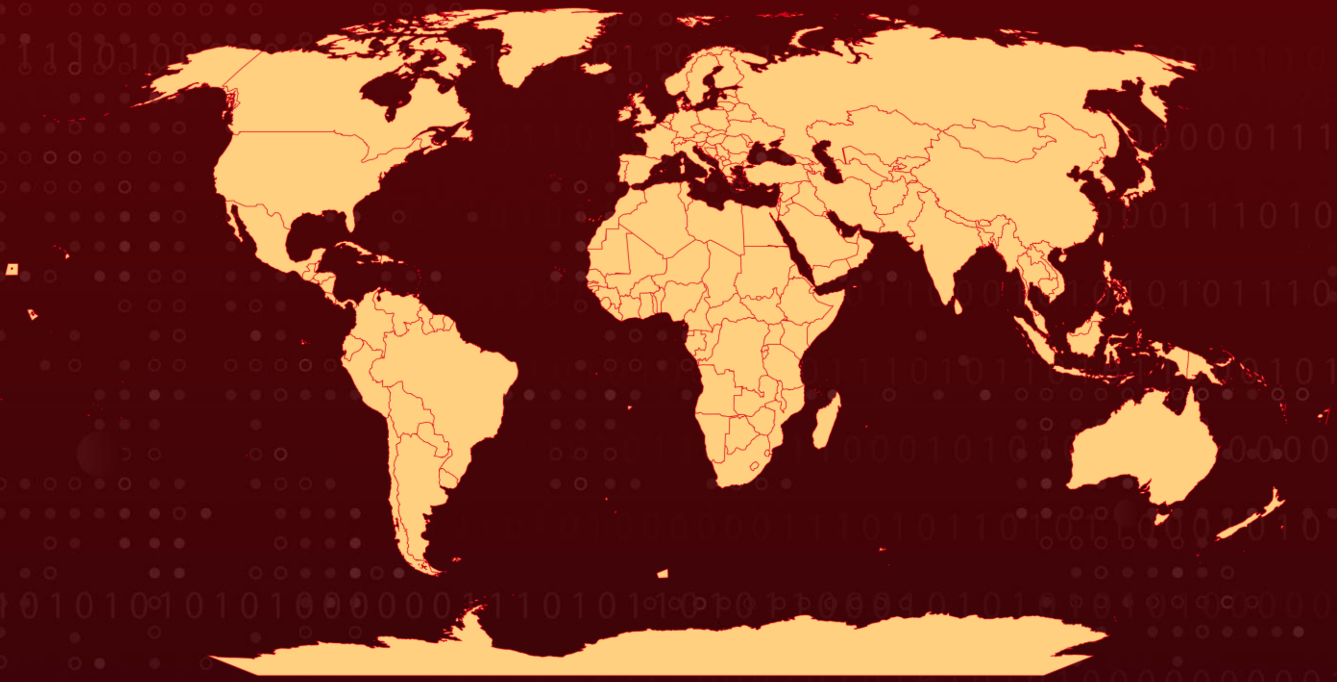
FortiClient EMS Vulnerability Exploited in Connect:fun Campaign

Date of Publication	Admiralty Code	TA Number
April 16, 2024	A1	TA2024148

Summary

Attack Began: March 23, 2024
Targeted Countries: Worldwide
Threat Actor: Unknown
Campaign Name: Connect:fun
Affected Platform: Fortinet FortiClientEMS
Attack: A cyber campaign dubbed Connect:fun targets organizations with vulnerable Fortinet FortiClient EMS systems. Exploiting CVE-2023-48788, attackers gain remote access, deploying tools like ScreenConnect and Powerfun, posing significant threats globally.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-48788	Fortinet FortiClientEMS SQL Injection Vulnerability	Fortinet FortiClientEMS	✗	✓	✓

Attack Details

#1 A cyberattack campaign dubbed Connect:fun has surfaced, aiming at organizations relying on Fortinet's FortiClient EMS, which harbors a critical vulnerability known as CVE-2023-48788. Recently, a media company was targeted in such an attack, revealing the dire consequences of this vulnerability's exploitation. This vulnerability allowed attackers to remotely take control of the system and potentially cause significant damage.

#2 The attackers used a publicly available exploit to gain remote code execution (RCE) capabilities, essentially giving them the ability to run malicious code on the media company's system. The investigation revealed that the attackers used manual exploitation techniques, suggesting a targeted attack rather than a widespread automated one.

#3 Once they gained access, the attackers wasted no time deploying tools to maintain control of the system. They downloaded ScreenConnect, a popular remote access software, likely to establish a persistent connection. Additionally, they attempted to download a powerful tool called Metasploit's Powerfun script, which is often used by attackers to perform actions after they have initially compromised a system. The threat actor's infrastructure spans across multiple countries, indicating a sophisticated and persistent threat.

Recommendations

Apply Patch: Ensure that all Fortinet FortiClient EMS systems are updated with the latest patches provided by Fortinet to address the CVE-2023-48788 vulnerability. Regularly check for and apply security updates and patches to keep systems protected against known vulnerabilities.

Employ Web Application Firewalls (WAF): Utilize web application firewalls to filter and monitor HTTP traffic to and from FortiClient EMS systems. WAFs can block potentially malicious requests and help prevent unauthorized access or exploitation of vulnerabilities like CVE-2023-48788.

Enhance Endpoint Security: Strengthen endpoint security measures by deploying endpoint protection platforms (EPP) and endpoint detection and response (EDR) solutions. These tools can help detect and respond to malicious activity on individual devices, providing an additional layer of defense against threats targeting FortiClient EMS systems.

Network Segmentation: Implement network segmentation to isolate critical systems like FortiClient EMS from other parts of the network. By segmenting the network, organizations can limit the scope of potential attacks and minimize the impact of security incidents.

Continuous Monitoring and Logging: Maintain thorough monitoring of system and network activities, and keep detailed logs of user actions, especially those involving critical processes and file access. Regularly review these logs for suspicious activities.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**TA0001** Initial Access	**TA0005** Defense Evasion
TA0011 Command and Control	**TA0003** Persistence	**T1218** System Binary Proxy Execution	**T1059** Command and Scripting Interpreter
T1588 Obtain Capabilities	**T1203** Exploitation for Client Execution	**T1588.005** Exploits	**T1588.006** Vulnerabilities
T1059.001 PowerShell	**T1105** Ingress Tool Transfer	**T1133** External Remote Services	**T1218.007** Msiexec
T1027 Obfuscated Files or Information	**T1190** Exploit Public-Facing Application	**T1219** Remote Access Software	**T1059.003** Windows Command Shell
T1027.010 Command Obfuscation			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv6	2a02:4780:a:952:0:1e10:e79b[:]1
IPv4	141[.]136[.]43[.]188 144[.]202[.]21[.]16 185[.]56[.]83[.]82 95[.]179[.]241[.]10 45[.]77[.]160[.]195 216[.]245[.]184[.]86
IPv4: PORT	10[.]0[.]40[.]63[:]8013
URLs	hxxp[:]//45.227.255[.]213:20201 hxxp[:]//68[.]178.202.116
Domains	mci11[.]raow[.]fun jxqmwbgxygkyftpxykdk8cfkq1hy371pz.oast[.]fun
Host name	VULTR-GUEST

Patch Details

Patched versions of Fortinet FortiClientEMS:
Upgrade to 7.2.3 or above
Upgrade to 7.0.11 or above

Links:
https://fortiguard.fortinet.com/psirt/FG-IR-24-007

References

https://www.forescout.com/blog/connectfun-new-exploit-campaign-in-the-wild-targets-media-company/

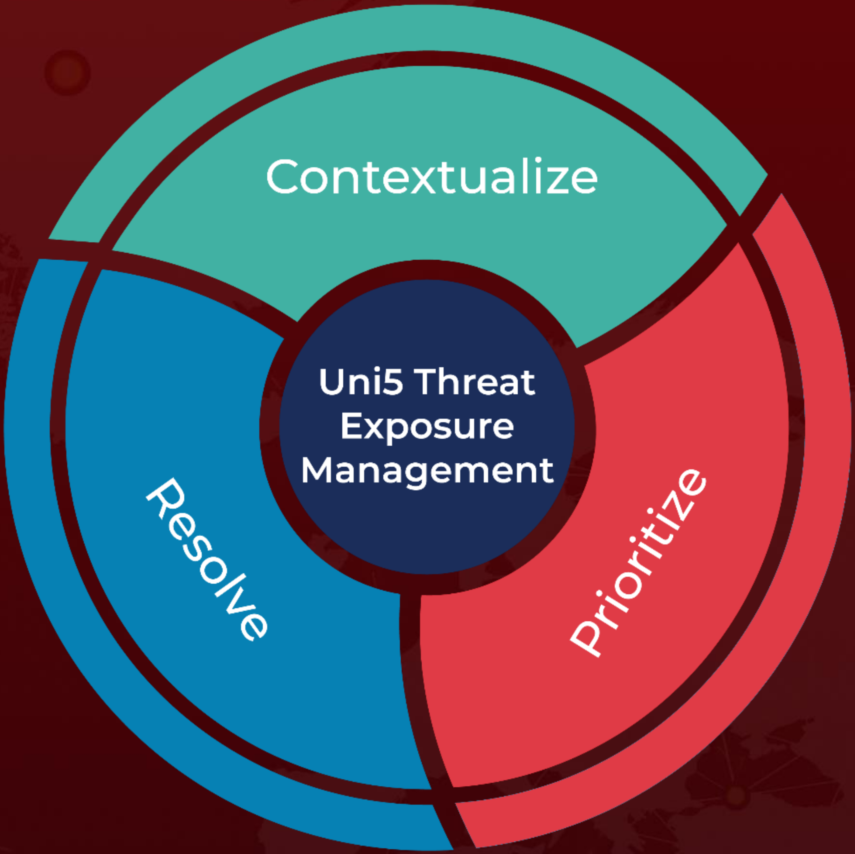
https://www.forescout.com/resources/connectfun-threat-briefing/

https://www.hivepro.com/threat-advisory/fortinet-releases-patches-for-critical-vulnerabilities-in-various-products/

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

April 16, 2024 • 5:30 AM

More at www.hivepro.com