Hive Pro

Threat Level

Red

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

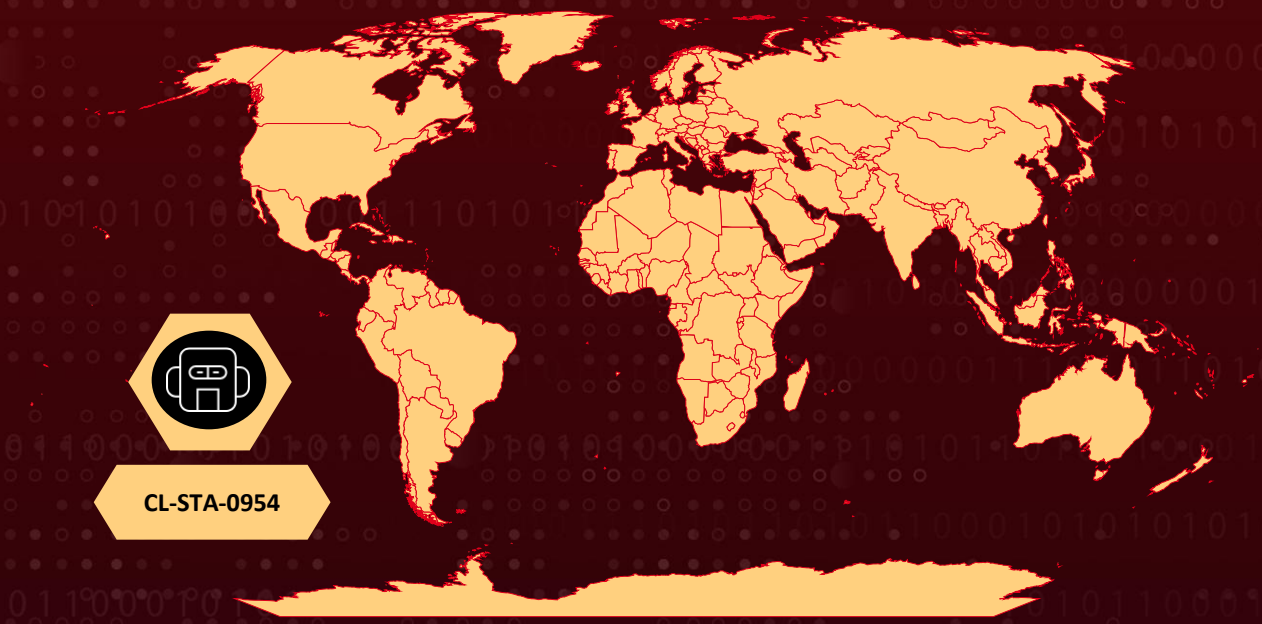
# PEERSTITCH: The FortiGate Implant That Hides Inside Trusted Processes


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| October 16, 2026 | A1 | TA2026304 |

# Summary

**First Seen:** September 2024
**Targeted Regions:** Worldwide
**Targeted Products:** Fortinet FortiManager, Fortinet FortiGate, Fortinet FortiOS, Fortinet FortiPAM, Fortinet FortiProxy, Fortinet FortiSwitchManager
**Targeted Industries:** Telecommunications, Managed Service Providers
**Threat Actor:** CL-STA-0954 (aka UNC5820)
**Malware:** PEERSTITCH
**Attack:** A suspected nation-state cluster tracked as CL-STA-0954 broke into a telecommunications managed service provider by exploiting the FortiJump flaw in a central FortiManager appliance. From that single box, the attackers walked away with the running configurations, credentials, and cryptographic trust material for more than 500 managed FortiGate firewalls, including devices protecting client networks. They later returned with stolen credentials, abused a FortiOS path traversal flaw to gain root, and deployed PEERSTITCH, a memory-resident ARM64 implant that writes nothing to disk, opens no ports and makes no outbound connections of its own. Instead it stitches two legitimate FortiOS daemons together through shared process memory and uses their traffic as cover, letting the attackers wave through tagged VPN sessions that FortiOS would normally reject.

## Attack Regions



## CVEs

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | CISA KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2025-61624 | Fortinet FortiOS CLI Path Traversal Vulnerability | Fortinet FortiOS, FortiPAM, FortiProxy, FortiSwitch Manager | ✗ | ✗ | ✓ |
| CVE-2024-47575 | FortiJump (Fortinet FortiManager Missing Authentication Vulnerability) | Fortinet FortiManager | ✓ | ✓ | ✓ |

# Attack Details

**#1**

A state-backed actor has been caught abusing a Fortinet FortiOS weakness to plant PEERSTITCH, a memory-resident ARM64 implant not documented until now. The attackers started at the top of the network rather than at its edge. CL-STA-0954 exploited CVE-2024-47575, better known as FortiJump, against the victim's central FortiManager appliance. The flaw lets an unauthenticated attacker run commands through the FMG-Access channel on TCP port 541. They used it to register a rogue virtual FortiGate named localhost, serial number FMG-VMTM23017412, from 45[.]32[.]41[.]202 and later 198[.]199[.]122[.]22. Moments after that, they built a configuration archive called .tm on the appliance and pulled it out of the network.

**#2**

That archive was the real prize. It held the running configurations of more than 500 managed FortiGate firewalls, the central management databases, an inventory of serial numbers paired with public IP addresses, internal topology maps, and the certificates and private keys that hold the trust between the manager and every device it controls. The stored passwords were only reversibly encrypted, and it was confirmed that administrative and SSL/VPN credentials could be cracked straight out of the stolen files.

**#3**

After a long quiet period, the attackers came back and started listening. They used the compromised FortiManager to push unauthorized packet capture rules to managed firewalls, targeting cleartext HTTP, RADIUS, LDAP and TFTP traffic to collect credentials and map the network. Then they logged in as legitimate users, opening SSL/VPN sessions from 23[.]240[.]77[.]233 and 47[.]18[.]167[.]159. That put them inside internal management segments, but still inside the restricted FortiOS admin shell, so they exploited CVE-2025-61624 to break out. The system.auto-script engine does not sanitize object names, so an auto-script object carrying a traversal name wrote a loader outside its intended directory and ran it as root.

**#4**

The loader downloaded five files, including JavaScript and WebAssembly components and a native ARM64 binary saved as lldprx. That binary is PEERSTITCH, and it runs exactly once. It finds the running /bin/miglogd logging daemon and /bin/iked VPN daemon, attaches to both with ptrace, freezes them, allocates a 16 KB read-write-execute memory region in each, and writes its payload there. It then patches three fixed offsets to suppress tamper detection and redirects execution into the hook. Afterwards, it deletes its own file and kills the staging process, leaving nothing on disk. The two hooks talk to each other by writing directly into each other's process memory, watching passing traffic for the markers 8550 and 169.254.0.1 and passing session tags across. When iked later sees a tagged VPN session, it takes an alternate code path and skips normal FortiOS security checks.

**#5**

The attackers also built a backup way in and then cleaned up behind themselves. They reconfigured the Apache mod_md module on FortiGate so that certificate validation ran Node.js with instructions pulled from their own ACME server on 23[.]240[.]77[.]233, spawning an SSH reverse shell that Apache kept renewing on its own. Separately, they used the stolen trust material to impersonate the FortiManager over FGFM and pulled configurations from other firewalls using an account named FortiGateCloud that the victim had never created. Finally they killed the logging daemons, cleared crash logs, deleted the rogue accounts and auto-script objects, and overwrote the malicious Apache config with harmless-looking text.

# Recommendations

**Patch FortiOS Against CVE-2025-61624:** Apply the fixes described in FortiGuard advisory FG-IR-26-122 to FortiOS, FortiPAM, FortiProxy and FortiSwitchManager. Until that patch is in place, any administrative account on the appliance is effectively a root account.

**Patch FortiManager Against FortiJump:** Update FortiManager per FG-IR-24-423 to close CVE-2024-47575. If the appliance was internet-exposed before patching, treat it as compromised rather than fixed, because patching removes the entry point but not what already walked out.

**Rotate Everything the Manager Held:** Assume every credential and certificate stored on a compromised FortiManager is in an attacker's hands. Rotate administrative, local, and SSL/VPN passwords, reissue device certificates and private keys, and regenerate the FGFM trust material for every managed firewall. This material stays valid until it is rotated, patched, or not.

**Hunt for the Memory Implant:** PEERSTITCH only exists in RAM, so look there. Inspect /proc/<pid>/maps for /bin/miglogd and /bin/iked for anonymous 16,384-byte regions carrying rwxp permissions, and verify text segment integrity at base+0x106F7B8, base+0x1072E20 and base+0x109A570 for the NOP pattern 0xAA0003E0.

**Audit Auto-Script Objects for Traversal Strings:** Review FortiOS configuration revisions for any system.auto-script object whose name contains ../ sequences. The attackers deleted theirs after execution, so historical revisions and configuration backups matter more than the current running config.

**Inspect Apache mod_md Configuration on FortiGate:** Verify that /tmp/apache2/conf/md-acme.conf has not been altered to point at an unfamiliar ACME directory, that MDChallengeDns01 is not mapped to /bin/node, and that MDRenewMode has not been forced to always.

**Isolate Management Interfaces Behind Zero Trust:** FMG-Access and FGFM on TCP port 541 should never be reachable from the internet. Restrict management plane access to a dedicated out-of-band network with explicit allowlisting, since this intrusion turned one reachable management port into visibility over 500 firewalls.

# Potential MITRE ATT&CK TTPs

| Tactic | Technique | Sub-technique |
|---|---|---|
| Initial Access | T1190: Exploit Public-Facing Application | |
| | T1133: External Remote Services | |
| | T1078: Valid Accounts | T1078.003: Local Accounts |
| Execution | T1059: Command and Scripting Interpreter | T1059.007: JavaScript |
| Persistence | T1543: Create or Modify System Process | |
| Privilege Escalation | T1068: Exploitation for Privilege Escalation | |
| | T1055: Process Injection | T1055.008: Ptrace System Calls |
| Defense Evasion | T1562: Impair Defenses | T1562.001: Disable or Modify Tools |
| | T1070: Indicator Removal | T1070.002: Clear Linux or Mac System Logs |
| | | T1070.004: File Deletion |
| | T1036: Masquerading | |
| | T1014: Rootkit | |
| | T1211: Exploitation for Defense Evasion | |

| Tactic | Technique | Sub-technique |
|---|---|---|
| Credential Access | T1110: Brute Force | T1110.002: Password Cracking |
| | T1040: Network Sniffing | |
| | T1552: Unsecured Credentials | T1552.001: Credentials In Files |
| | T1649: Steal or Forge Authentication Certificates | |
| Discovery | T1046: Network Service Discovery | |
| Lateral Movement | T1021: Remote Services | |
| Collection | T1005: Data from Local System | |
| | T1074: Data Staged | T1074.001: Local Data Staging |
| | T1602: Data from Configuration Repository | |
| Command and Control | T1071: Application Layer Protocol | T1071.001: Web Protocols |
| | T1105: Ingress Tool Transfer | |
| | T1219: Remote Access Tools | |

| Tactic | Technique | Sub-technique |
|---|---|---|
| Command and Control | T1205: Traffic Signaling | |
| | T1008: Fallback Channels | |
| Exfiltration | T1041: Exfiltration Over C2 Channel | |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA256 | b9fb0b27ddd59b58d3ae53c7227298a3e0de1e6f868b9429ae21533bb9cd1e70, 829b1cd270b30565739a478441833f49f10a49bd06f0d18cc96c8ae4a0431f11, bd064244dad748cf2a44074bee56f5bfab4a2b18ee944b75d1b3febd4c1fe02a, 9c4c4436ff5cdf0d6d68f5108031cbf3708a095cde4ef8c09316af7a7110437e, fc1b10c58057ef9f1f9a1e2a3d4a1c89f43b0ead451398c70ed7a6e0312b36ee, f84eea718526706afdf2d1a2774fab76ecb11c18fb61995a37be8249c5e379ab, b7ae166fd49a7ecfe6322a80b8aa56d6aa0825d8f5d106dab2e4fb7d14ce15a8, 8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92 |
| IPv4 | 23[.]240[.]77[.]233, 47[.]18[.]167[.]159, 45[.]32[.]41[.]202, 198[.]199[.]122[.]22 |
| URL | hxxp[:]//23[.]240[.]77[.]233[:]8085/pM.js, hxxp[:]//47[.]18[.]167[.]159[:]8085/pM.js, hxxp[:]//23[.]240[.]77[.]233[:]8084/directory, hxxp[:]//23[.]240[.]77[.]233[:]8084/acme/new-acct, hxxp[:]//23[.]240[.]77[.]233[:]8084/acme/order/11111, hxxp[:]//23[.]240[.]77[.]233[:]8084/acme/authz/1, hxxp[:]//23[.]240[.]77[.]233[:]8084/acme/finalize/61924744/774083503 |

| TYPE | VALUE |
| --- | --- |
| Filename | lldprx,<br>pM.js,<br>index.js,<br>index.wasm,<br>ipssem.js |
| File Path | ../../../../setup,<br>../../tmp/apache2/conf/md-acme.conf |

## Patch Links

CVE-2024-47575: https://www.fortiguard.com/psirt/FG-IR-24-423

CVE-2025-61624: https://fortiguard.fortinet.com/psirt/FG-IR-26-122

## References

https://unit42.paloaltonetworks.com/fortimanager-cve-2024-47575-peerstitch-malware/

https://hivepro.com/threat-advisory/unc5820-exploits-critical-fortimanager-zero-day-to-hijack-enterprise-networks/

# 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 Demo of **HivePro**.

REPORT GENERATED ON

**October 16, 2026 • 11:00 AM**

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com