

CYBERSECURITY ADVISORY

TLP: CLEAR

JCSA-20261006-01

Co-Authored by:



FortiBleed Operations Continue Targeting Exposed Systems Leading to Reports of Lockouts

Publication: October 6, 2026

U.S. Federal Bureau of Investigation

United States Secret Service

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact the FBI's [Internet Crime Complaint Center \(IC3\)](#), your [local FBI field office](#), and/or CISA's 24/7 Operations Center at contact@cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA-client requirements or cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.

This document is distributed as TLP: CLEAR. Recipients may only share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see Traffic Light Protocol (TLP) Definitions and Usage.

TLP: CLEAR

Advisory at a Glance

Title	FortiBleed Operations Continue Targeting Exposed Systems Leading to Reports of Lockouts
Original Publication	October 6, 2026
Executive Summary	This joint cybersecurity advisory was developed by the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (USSS) to provide information and disseminate indicators of compromise (IOCs) related to the ongoing FortiBleed compromise. FortiBleed is an active, global credential-compromise campaign targeting internet-facing Fortinet FortiGate firewalls and secure socket layer (SSL) virtual private network (VPN) gateways, with SOCRadar verifying more than 86,644 compromised devices across 194 countries¹. This advisory provides details on the campaign exploits reused or leaked credentials and a legacy SHA-256 password storage, enabling threat actors to harvest and crack authentication data at scale.
Key Actions	▪ Reduce your attack surface and lock down management access. Restrict external management of your devices via trusted hosts (good), a local-in policy (better), or remove internet administration altogether (best). ▪ Terminate all admin and VPN sessions and reset credentials. Terminate all active administrative sessions. Reset all Fortinet VPN and administrative passwords, especially on internet-facing systems, and enforce strong password policies. ▪ Enable phishing-resistant multifactor authentication (MFA). Require phishing-resistant MFA on all remote access and administrative accounts and ensure it is enforced on all external gateways and administrative interfaces.
Intended Audience	Organizations: This cybersecurity advisory applies to all 16 sectors, chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste sector, transportation systems, and water and wastewater sector. Roles: This cybersecurity advisory focuses on the indicators of compromise and mitigation strategies related to the Fortibleed attach chain, making the target audience defensive cybersecurity analysts, vulnerability analysts, and Chief Information Security Officers (CISO) of organizations.

Introduction

This joint cybersecurity advisory was developed by the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (USSS) to provide information and disseminate indicators of compromise (IOCs) related to the ongoing FortiBleed compromise. FortiBleed is an active, global credential-compromise campaign targeting internet-facing Fortinet FortiGate firewalls and secure socket layer (SSL) virtual private network (VPN) gateways, with SOCRadar verifying more than 86,644 compromised devices across 194 countries². The campaign exploits reused or leaked credentials and legacy SHA-256 password storage, enabling threat actors to harvest and crack authentication data at scale. Initial findings indicate attackers are continuing to scan internet-exposed Fortinet firewalls using previously obtained compromised credentials. Affected organizations may find themselves locked out of their systems if threat actors disable accounts or change passwords, requiring remediation steps beyond standard patching and password resets. In addition, the FortiBleed attack chain has been observed as an initial entry point for ransomware affiliates. The FBI and USSS encourage organizations to implement the mitigations outlined in this advisory to help minimize the potential for impact from the FortiBleed attack chain.

Technical Details

Note: This advisory uses the [MITRE ATT&CK® Matrix for Enterprise](#) framework, version 19.1. See the MITRE ATT&CK Tactics and Techniques section of this advisory table of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques.

Overview

FortiBleed refers to a credential-harvesting and access-broker operation whose internal workflow became visible only after the threat actors unintentionally exposed their own backend server. The open directory revealed a mature, multi-stage campaign targeting FortiGate SSL VPN appliances, harvesting credentials at scale, and cracking them using a distributed graphics processing unit (GPU) cluster. The recovered tooling and datasets provide a rare, end-to-end view of how the operators identified targets, validated stolen credentials, and expanded access inside victim networks. The following points summarize the attackers' progression based on the artifacts left behind.³

- Attackers began by scanning [\[T1595\]](#) the internet for exposed [\[T1190\]](#) FortiGate SSL VPN portals, using automated scripts to identify reachable devices and harvestable authentication surfaces.
- They collected large volumes of credentials and authentication artifacts using credential stuffing [\[T1110.004\]](#) and password spraying [\[T1110.003\]](#) attacks based on prior Fortinet leak dumps and infostealer logs.
- Exfiltrated [\[T1041\]](#) password hashes obtained via credential dumping [\[T1003\]](#) were funneled into a GPU-accelerated cracking cluster to perform offline password cracking [\[T1110.002\]](#), where

Hashcat and Hashtopolis¹ orchestrated distributed jobs to convert stolen data into usable plaintext credentials.

- Cracked credentials were enriched, sorted, and validated, with scripts filtering out honeypots, mapping organizations, and prioritizing high-value targets based on revenue and network structure. New administrative accounts were created [\[T1136.001\]](#) on the firewall to maintain persistence.
- With verified credentials [\[T1078\]](#) in hand, attackers moved into victim environments, conducting Active Directory enumeration [\[T1087\]](#) and password spraying to expand access and identify privileged accounts.
- The operation culminated in packaging and selling access, with working VPN configurations and target lists indicating the group's role as an initial-access broker supplying compromised networks to downstream threat actors.

Potential Lockout

Based on initial responses, some victims may get locked out of their Fortinet devices if the threat actor either deletes or changes the password for original accounts on the system [\[T1531\]](#). During the initial intrusion, threat actors create new accounts not previously on the device. In certain cases, threat actors delete existing accounts to block organizations from accessing affected devices and to maintain persistence on the system while attempting lateral movement within the environment.

Indicators of Compromise

IP Addresses in Victim Logs

Initial responses revealed ongoing scanning activity on exposed Fortinet firewalls. Threat actors use a combination of Internet Protocol (IP) addresses for their infrastructure to include their Command and Control (C2) servers, Relay Nodes, performing scanning activities, and using Hashtopolis. IP address 45.154.12.132 was seen in instances as a C2 server, with IP addresses 154.202.59.169 and 103.27.186.156 as proxy nodes used by the threat actors to obfuscate their presence, and 45.155.250.158 as a beacon relay. Threat actors use multiple different ports, including 4332 and 4432, but usually beaconing to (Hypertext Transfer Protocol Secure) HTTPS. In addition, IP addresses 193.8.187.2, 193.8.187.42, and 85.11.187.8 were seen facilitating the FortiBleed attack chain, with IP address 85.11.187.8 being used for the Hashtopolis tool.⁴ The following IP addresses have been identified as currently conducting brute force attacks or have successfully authenticated using a compromised account.

¹ (U) Note: Hashtopolis is an open-source platform used to distribute password cracking capabilities across computing and network resources.

Table 1: Observed IP Addresses

IP Addresses Used by Threat Actors	Dates Observed
104.28.155.27	06/19/26 to 06/20/26
185.136.15.43	06/27/26 to 07/23/26
185.136.15.66	06/27/26 to 07/23/26
185.199.199.56	06/25/26
193.8.186.33	06/18/26 to 07/20/26
45.227.254.210	06/18/26 to 07/23/26
77.91.118.10	06/18/26 to 07/05/26
80.75.212.113	06/26/26 to 07/05/26
87.251.64.13	06/18/26 to 07/22/26
87.251.64.16	06/18/26 to 07/20/26
87.251.64.17	06/18/26 to 07/20/26
87.251.64.44	07/04/26
66.175.220.111	07/17/26 to 07/19/26

Table 1: Observed IP addresses identified currently conducting brute force attacks or have conducted successful authentication using compromised accounts. The authoring agencies recognize that infrastructure used for malicious activity may be hosted on cloud or virtualized platforms where IP addresses can be dynamically or temporarily assigned. As a result, an address associated with malicious activity at one point in time may later be reassigned to benign services. Accordingly, these indicators should be interpreted as historically observed infrastructure within the activity window and should be corroborated with current network telemetry or additional intelligence sources when used for defensive or investigative purposes.

Compromised Account Names

After initial access is gained, threat actors begin adding accounts to the system. Initial investigations revealed the creation of multiple new accounts to maintain persistence within the network. It is recommended that organizations review all Fortinet accounts and verify their legitimacy. In some instances, threat actors may have exploited SSH if the port was open on the firewall. The following list of commonly identified compromised account names is provided to assist with the review process.

Table 2: Compromised Account Names

Compromised Account Names		
adminin	fortiAdmin	forticloud-sync
admin	fgtsecure	pakedge
forticloud-tech	districtadmin	system_config
gttadmin	roadmin	itadmin
Technical_support	adminsslvpn	IT_Manager
my_admin	support_fortinet	fgtsec
forti_support2		

Table 2: Observed usernames of compromised accounts found on victim systems after threat actors performed initial intrusion.

Ransomware Connection with FortiBleed Attack Chain

Reporting indicates initial access brokers (IABs), utilizing the FortiBleed attack chain, have provided further access to ransomware affiliates, currently including INC/Lynx ransomware and Payload ransomware.

MITRE ATT&CK Tactics and Techniques

See **Table 3** to **Table 9** for all referenced threat actor tactics and techniques in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see Cybersecurity and Infrastructure Security Agency (CISA) and MITRE ATT&CK's [Best Practices for MITRE ATT&CK Mapping](#) and CISA's [Decider Tool](#).

Table 3: Resource Development

Technique Title	ID	Use
Acquire Infrastructure	T1583	Adversaries rented GPU infrastructure to support large-scale cracking of stolen password hashes.

Table 4: Initial Access

Technique Title	ID	Use
Active Scanning	T1595	Adversaries scanned the internet to identify internet-facing FortiGate SSL-VPN portals for potential compromise.
Exploit Public-Facing Application	T1190	Adversaries targeted publicly exposed FortiGate infrastructure.
Password Spraying	T1110.003	Adversaries attempted a small set of common passwords across many accounts to obtain valid credentials.
Credential Stuffing	T1110.004	Adversaries used credentials obtained from prior breaches to authenticate FortiGate devices and VPN portals.

Table 5: Credential Access

Technique Title	ID	Use
Credential Dumping	T1003	Adversaries extracted FortiOS user databases and session tokens from compromised devices to obtain additional credentials.

Table 6: Persistence

Technique Title	ID	Use
Create Local Accounts	T1136.001	Adversaries created new administrative accounts on FortiGate devices to maintain persistent access.

Table 7: Discovery

Technique Title	ID	Use
Account Discovery	T1087	Active Directory account enumeration was reported to identify users and privileges for further lateral movement.

Table 8: Exfiltration

Technique Title	ID	Use
Exfiltration Over C2 Channel	T1041	Compromised devices continuously transmitted harvested credentials to attacker-controlled servers, feeding the scanning and cracking pipeline.

Table 9: Impact

Technique Title	ID	Use
Account Access Removal	T1531	Adversaries intentionally locked, disabled, or altered account access so legitimate administrators could not log in.

Incident Response

If a potential compromise is detected, organizations should take the following actions:

1. **Determine which hosts were compromised and isolated them** by quarantining or taking them offline.
2. **Initiate threat hunting activities to scope the intrusion**—collect and review relevant artifacts, logs, and other data to identify threat actor TTPs, compromised devices and accounts, a timeline of activity, etc.
3. **Report the compromise to the FBI, USSS, and other agencies** as appropriate (see Contact Information for details).
4. **Apply eviction countermeasures**, including those listed below, to contain the incident and eradicate the threat actor from the network (**Note:** Start applying countermeasures after collecting enough threat hunting data to inform effective countermeasure selection; this will likely overlap with threat hunting activities):
 - a. Use CISA's [Eviction Strategies Tool](#) to assemble countermeasures for a systematic eviction plan—the tool comprises **Playbook-NG** (a web application) and **COUN7ER** (a database of post-compromise countermeasures mapped to adversary TTPs).
 - i. Use Playbook-NG and COUN7ER together to assemble a systematic eviction plan, or playbook, that leverages distinct countermeasures to contain and evict cyber threat actors. The playbook features a list of recommended response actions based on threat actor TTPs and includes each action's intended outcome, preparatory steps, and associated risks. For more information, see CISA's [Eviction Strategies Tool Fact Sheet](#).
5. **Harden the network to prevent additional malicious activity** (see **Mitigations** for guidance).

Mitigations

Due to the potential damage this attack chain can lead to with lockout and ransomware, the FBI and USSS encourage organizations to review the following mitigations to help defend against this malicious cyber activity, impacting all Fortinet customers with exposed gateways:⁵

- Reduce your attack surface and lock down management access. Restrict external management of your devices via trusted hosts (good), a local-in policy (better), or remove internet administration altogether (best).
- Terminate all admin and VPN sessions and reset credentials. Terminate all active administrative sessions. Reset all Fortinet VPN and administrative passwords, especially on internet-facing systems, and enforce strong password policies.
- Enable phishing-resistant multifactor authentication (MFA). Require phishing-resistant MFA on all remote access and administrative accounts and ensure it is enforced on all external gateways and administrative interfaces.
- Validate configuration. Review firewall and VPN users and other configuration for unauthorized changes. Preferably, compare configurations to a well-known configuration. Pay particular attention to the addition of unrecognized accounts. A list of well-known compromised account names has been mentioned in this report.
- Review logs. Review firewall, VPN, authentication, and domain controller logs for lateral movement, unusual access, suspicious accounts, or unauthorized configuration changes. A list of commonly identified IP addresses has been referenced in this report to assist with a review.
- Ensure secure credential storage. Confirm your organization's use of the Password-Based Key Derivation Function 2 (PBKDF2) algorithm to store administrator credentials and remove weaker legacy hashes per Fortinet's guidance. Refer to Fortinet's technical guidance on enforcing PBKDF2 as hash function for administrator accounts in FortiOS v7.2.11 and later.⁶

The authoring organizations recommend organizations investigate or vet IOCs prior to acting, such as blocking.

REST APIs

Representational state transfer (REST) application programming interface (API) keys can enable automated configuration, backup creation, and monitoring of FortiGate firewalls.⁷ Any unknown or unexpected keys may present a significant security risk. All API keys should be reviewed to confirm they have a valid purpose in the environment. It is recommended to identify and remove any unknown API keys and refresh all legitimate keys to ensure threat actors cannot leverage them for access.

Reporting

Your organization has no obligation to respond to or provide information to the authoring agencies in response to this joint advisory. If, after reviewing the information provided, your organization decides to provide information to FBI and/or USSS, reporting must be consistent with applicable state and federal laws.

The FBI and the USSS are interested in any information and IOCs that can be shared, including IP addresses and usernames used by the threat actors.

The authoring agencies do not encourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities.

Regardless of whether you or your organization have decided to pay the ransom, the FBI and USSS urge prompt reporting of cyber incidents to the FBI's [Internet Crime Complaint Center \(IC3\)](#), your [local FBI field office](#), and/or your [local USSS field office](#).

Contact Information

U.S. organizations are encouraged to report suspicious or criminal activity related to information in this advisory to the FBI, and/or USSS:

- File a claim with FBI's [Internet Crime Complaint Center \(IC3\)](#) or contact your local [FBI field office](#), and/or your [local USSS field office](#). When available, please include the following information regarding the incident:
 - Date, time, and location of the incident;
 - Type of activity;
 - Number of people affected;
 - Type of equipment used for the activity; and
 - Name of the submitting company or organization, and a designated point of contact.

Disclaimer

The information in this report is being provided “as is” for informational purposes only. FBI and USSS do not endorse any commercial products or services, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring agencies.

Version History

October 6, 2026: Initial version.

Notes

- ¹ <https://socradar.io/blog/fortibleed-fortinet-firewalls-compromised/>
- ² <https://socradar.io/blog/fortibleed-fortinet-firewalls-compromised/>
- ³ <https://www.cloudsek.com/blog/inside-the-fortibleed-open-directory-a-technical-analysis-of-what-the-attacker-left-behind>
- ⁴ <https://www.cloudsek.com/blog/inside-the-fortibleed-open-directory-a-technical-analysis-of-what-the-attacker-left-behind>
- ⁵ <https://www.fortinet.com/blog/psirt-blogs/analysis-of-reported-credential-compromise-of-fortigate-devices>
- ⁶ <https://community.fortinet.com/fortigate-3/technical-tip-enforcing-pbkdf2-as-hash-function-for-administrator-accounts-in-fortios-v7-2-11-and-later-220652>
- ⁷ <https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/399023/rest-api-administrator>