FortiBleed Campaign Exposes Thousands of Fortinet Firewall Administrator Credentials

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

A campaign known as FortiBleed has exposed working administrator credentials associated with thousands of internet-facing Fortinet FortiGate firewalls and SSL VPN gateways worldwide.

The compromised credentials could allow threat actors to gain unauthorized access to firewall management interfaces and remote access services used by organizations across multiple industries.

Overview

Fortinet FortiGate firewalls are commonly used to protect enterprise networks and provide secure remote access through SSL VPN services. A campaign known as **FortiBleed** has exposed working administrator credentials associated with thousands of internet-facing FortiGate firewalls and VPN gateways.

Threat actors obtained FortiGate configuration files containing administrator credential hashes and used GPU-powered cracking infrastructure to recover valid credentials. Databases containing verified administrator usernames and passwords for thousands of organizations were later discovered online.

Affected Products

- Fortinet FortiGate Firewalls
- Fortinet SSL VPN Gateways
- Internet-facing FortiGate management interfaces
- Organizations using legacy administrator password hashes following FortiOS upgrades

FortiBleed has been linked to a Russian-speaking threat group (not publicly known). The campaign has affected organizations in 194 countries, with the highest concentrations of exposed devices reported in India, the United States, Taiwan, and Mexico. Impacted sectors include information technology, telecommunications, manufacturing, construction, government, defense, and professional services.

Organizations with exposed credentials are vulnerable to unauthorized access through firewall management interfaces and VPN services. Successful access may allow threat actors to modify security settings, create accounts, disable security controls, monitor

network traffic, harvest additional credentials, and gain access to internal systems. There has also been activity involving access to internal Active Directory environments following successful compromises.

Fortinet stated that FortiBleed is not associated with a newly disclosed vulnerability and does not currently have an assigned CVE or CVSS score. The campaign relies on compromised credentials and cracked password hashes. There is currently no patch available because the activity does not involve exploitation of a software vulnerability.

Aspire Protects

- Immediately reset all FortiGate administrator passwords.
- Reset SSL VPN credentials, particularly for internet-facing systems.
- Restrict firewall management interfaces to trusted internal networks whenever possible.
- Verify all administrators have logged in following FortiOS upgrades to ensure PBKDF2 password hashing is applied.
- Review firewall, VPN, and authentication logs for unauthorized access and suspicious login activity.
- Investigate unexpected administrative accounts, configuration changes, and policy modifications.

TTPs

Initial Access

- Valid Accounts [T1078] – Threat actors use compromised administrator and VPN credentials to gain unauthorized access to FortiGate devices and enterprise networks.

Credential Access

- Brute Force [T1110] – Attackers crack credential hashes to recover valid administrator passwords.
- Credentials from Password Stores [T1555] – Password hashes extracted from FortiGate configuration files are used to recover administrative credentials.

Discovery

- Network Service Scanning [T1046] – Automated scanning is used to identify internet-facing FortiGate firewalls and VPN services.

Collection

- Network Sniffing [T1040] – Compromised devices may be used to monitor network traffic and collect additional credentials.

Lateral Movement

- Remote Services [T1021] – Stolen VPN and administrative credentials may be used to access internal systems and move throughout the network.

Persistence

- Account Manipulation [T1098] – Administrative access may be used to create or modify accounts for continued access.

Defense Evasion

- Impair Defenses [T1562] – Attackers may modify firewall policies, disable security controls, or alter logging configurations.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Organizations across multiple sectors have been affected, including:

- Public Sector
- Professional Services
- Construction
- Manufacturing
- Defense
- Information Technology
- Telecommunications

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.

  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

LinkedIn.com/posts/vdyachenko_massive-fortinetfortigate-bruteforceactive

Cybercriminals allegedly hacked tens of thousands of Fortinet firewalls used by major companies all over the world | TechCrunch

Active FortiBleed Campaign Impacting Fortinet Devices Across 194 Countries | Arctic Wolf