ADVISORY:
Fortinet "Fortibleed" Compromise
18 JUNE 2026

Overview

"Fortibleed" is a global, large-scale credential exposure and exploitation campaign targeting Fortinet firewalls and VPN appliances. It is reported that admin credentials for over 70,000 Fortinet Fortigate firewalls have been exposed, with almost all firewall instances still active in organisations around the world.

Disclosed publicly on 17th June by security researcher, Bob Diachenko, this incident does not appear to be as a result of a single vulnerability, but rather a trove of data exposed on a server sitting on the open Internet. Further investigation has identified the credentials (including usernames, email addresses and plaintext passwords) as legitimate and originates from an active attacker infrastructure, and not just a passive leak.

Attackers possessing these credentials are actively exploiting live environments. They can remotely access the firewalls and, by extension, the internal network allowing them to modify security configurations and create backdoor administrative accounts on affected devices.

Scale of Compromise

- ~75,000 Fortinet firewall/VPN URLs included in the dataset
- Over 21,000 affected domains identified
- Potentially 30,000+ devices with confirmed working credentials
- Activity observer across over 190 countries

Global enterprises such as Samsung, Siemens and Oracle are confirmed to be included in the dataset. Government agencies and critical infrastructure are also affected with full network compromises already verified. Regardless of the size of your organisation, if you have active Fortinet products on your perimeter, it is essential to take action.

ADVISORY:
Fortinet "Fortibleed" Compromise

Recommended Action

Organisations using Fortinet products should:

- **Identify all internet-facing Fortinet assets** (Fortigate SS VPN, web admin interfaces etc.) – cyber security company, Hudson Rock, has released a lookup tool for affected domains (https://www.hudsonrock.com/fortinet), but **do not** rely solely upon this lookup for assurance.
- Immediately **rotate all credentials** for Fortinet admin accounts, VPN users and service accounts.
- **Enforce mandatory multi-factor authentication (MFA)** on all remote access, with strong, unique passwords.
- **Remove public exposure** of admin portals and management interfaces, and restrict access via IP allowlists or VPN-only access where possible.
- **Conduct retrospective analysis** – check VPN logs for unusual geolocations, admin activity, unknown accounts and privilege escalation events.
- Ensure all Fortinet instances are **patched for known vulnerabilities** and disable unused services.

If exposure is confirmed, treat your environment as potentially compromised. It is essential that you investigate for persistence mechanisms and lateral movement into internal systems.

References

More information and guidance can be found on the following pages:

HudsonRock - FortiBleed: 75,000 Fortinet Firewalls Compromised: Global Enterprises Exposed
Security Affairs - FortiBleed Exposes Admin Passwords for 75,000 Fortinet Firewalls