



FortiBleed: Fortinet Firewalls Credential Exposure and Vulnerability Disclosure

We are reaching out with an urgent security notice affecting Fortinet firewall and VPN environments. A large-scale attack campaign, now publicly known as "FortiBleed" — was disclosed on June 16-17, 2026, and is actively targeting organizations worldwide. We want to make sure you're informed and protected.

What is the Issue?

Attackers have been systematically breaking into Fortinet firewalls and VPN gateways at a massive scale, between 30,000 and 75,000 devices across 194 countries are confirmed affected.

Here is how the attack works:

1. Attackers scan the internet to find Fortinet devices that are publicly accessible.
2. They exploit a security flaw (CVE-2026-24858) to steal the device's configuration file, which contains encrypted passwords.
3. They crack those passwords offline, giving them working admin credentials.
4. They use those credentials to log into other Fortinet devices across the internet.
5. In some cases, they push fake Fortinet software updates through a second vulnerability (CVE-2026-35616) to install a password-stealing program called EKZ Infostealer onto managed endpoints. If your Fortinet device was internet-facing and unpatched, attackers may already have your admin credentials and could have used them.

You may be affected if your organization uses any of the following:

- Fortinet FortiGate firewalls
- Fortinet SSL-VPN gateways
- FortiClient Endpoint Management Server (EMS)

More information regarding this issue can be found on the links below.

- Fortinet PSIRT Advisories — <https://www.fortiguard.com/psirt>
- CISA KEV Catalog — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- SOCRadar: <https://socradar.io/blog/fortibleed-fortinet-firewalls-compromised/>
- Hudson Rock: [FortiBleed: 75,000 Fortinet Firewalls Compromised: Global Enterprises Exposed – Claim Your Ethical Disclosure](#)

What do you need to do?

1. Patch your devices : Security patches are available for both vulnerabilities.
2. Change All Fortinet Passwords: If your FortiGate device was unpatched before earlier this year, you should assume your admin and VPN credentials have been compromised and rotate them immediately.
3. Check for Suspicious Accounts : Look for any administrator accounts on your FortiGate that were not created by your team. This is a key sign of a successful breach.
4. Enable MFA: Ensure MFA is enabled on all remote access and administrative accounts on all external gateways and administrative interfaces.
5. Reduce Attack Surface: Lock down management access and make sure it is not accessible from the internet.

What is CloudWave doing?

- For customers that send their Fortigate logs to our 24/7 SOC, we have proactively reviewed the SOC Radar database ([FortiBleed Check — Find Leaked FortiBleed VPN Credentials | SOCRadar](#)) and have not found your domain or IP in the database.
- We have reviewed Fortigate logs in our SIEM and have provided customers certain logs to review to validate activity.
- Continuous monitoring for suspicious authentication activity

If you have infrastructure support with CloudWave and need assistance assessing your exposure or applying the patch, please contact us at 855-286-7787 or open a Service Request through the Customer Support Portal.