CYBER ADVISORY

Friday, June 19, 2026 **CAL-CSIC-202606-A-014**

Active "FortiBleed" Campaign Impacting Fortinet Firewalls and SSL VPN Interfaces

Active Campaign	Credential Harvest and Validation	Fortinet	Fully Automated

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of an active, large-scale breaching campaign targeting Fortinet devices – specifically involving Fortinet firewalls and VPN gateways. SOCRadar - a cybersecurity research entity, recently uncovered the campaign in which a threat actor has been systematically compromising the devices, building a database of working credentials. At this time, there are an estimated 86,644 compromised devices with 80,000 unique IPs, 22,405 Unique Domains across 194 countries.[1] Currently, there are no CVE numbers assigned to this "FortiBleed" campaign, as this campaign is still active, and is being actively investigated.[2] At the time of this writing, it is not a confirmed Fortinet zero-day exploit. This on-going campaign is best described as a Fortinet credential harvesting and validation campaign. Currently, there is no confirmed attribution to any specific threat actor.[2][3]

This large and active operation is built around a full automation process that self-sustains. The threat actor scans for public-facing Fortinet devices, tries to breach with a carefully curated list of known passwords compiled from a collection of credentials leaked from Fortinet devices in earlier incidents. Once a device is compromised, it is used to pass monitor traffic for additional credentials. Those credentials are then fed back into the automated scanner to compromise more devices.[3]

A cursory search in Shodan reveals over 6,500 public-facing Fortinet FortiGate devices of various degrees of VPN capabilities. The vast majority of these products belong to the communications (telecom) critical infrastructure (CI) sector.[4][5] Internal third-party sources reveal over 225 potentially vulnerable Fortinet FortiGate on-prem and cloud assets within California's internal networks.

The Cal-CSIC strongly recommends that any organization using Fortinet FortiGate SSL VPN devices or has Fortinet administrative interfaces with the internet, to review their logs, rotate credentials, enact multifactor authentication, update outdated firmware, and restrict management access to reduce attack surface.

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] SOCRadar; "FortiBleed Breach"; https://socradar.io/blog/fortibleed-fortinet-firewalls-compromised/; accessed 18 June 2026

[2] SOCRadar; "FortiBleed Breach: How 80,000+ Corporate Firewalls Were Quietly Compromised"; https://socradar.io/blog/fortibleed-fortinet-firewalls-compromised/; accessed 18 June 2026

[3] IT Knowledge Bases; FortiBleed: 75,000 Fortinet Firewalls Compromised — CVEs, Attack Chain, and How to Detect It"; https://itknowledgebases.com/fortibleed-fortinet-firewalls-compromised/; accessed 18 June 2026

[4] SOCRadar; " FortiBleed Breach: How 80,000+ Corporate Firewalls Were Quietly Compromised"; https://socradar.io/blog/fortibleed-fortinet-firewalls-compromised/; accessed 18 June 2026

[5] Shodan; "Facet Analysis"; https://www.shodan.io/search/facet?query=fortinet+fortigate+country%3A%22US%22+State%3ACA&facet=org; accessed 18 June 2026