CHUBB®

June 2026

BREAKING ALERT:

Chubb Vulnerability Alert System:

"Fortinet Critical Vulnerabilities and Global Credential Harvesting Campaign"

Chubb provides alerts to keep our policyholders informed of risks that may affect their organizations. Fortinet recently disclosed four critical vulnerabilities, (CVE-2026-39813, CVE-2026-39808, CVE-2026-25089, and CVE-2026-35616), affecting FortiSandbox and FortiClient EMS. In addition, on June 17 a widespread campaign targeting Fortinet firewall devices was disclosed. The campaign, leveraging previously harvested credentials, has successfully targeted more than 73,000 unique firewall URLs globally. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code.

Fortinet recommends immediately patching to the latest firmware, resetting all VPN user passwords, and enforcing multi-factor authentication (MFA).

Chubb's Cyber Risk Advisory Team is available to answer your questions and help mitigate cyber exposures like the one described above. To request advisory services, please click here.

For additional information, please contact cyber@chubb.com. You may also use Chubb's interactive tool Chubb Cyber Index® to access additional resources to help evaluate and address cyber risks your business may face.

Click here to learn more about Chubb's Cyber Services.

UK9136-HS 02/26