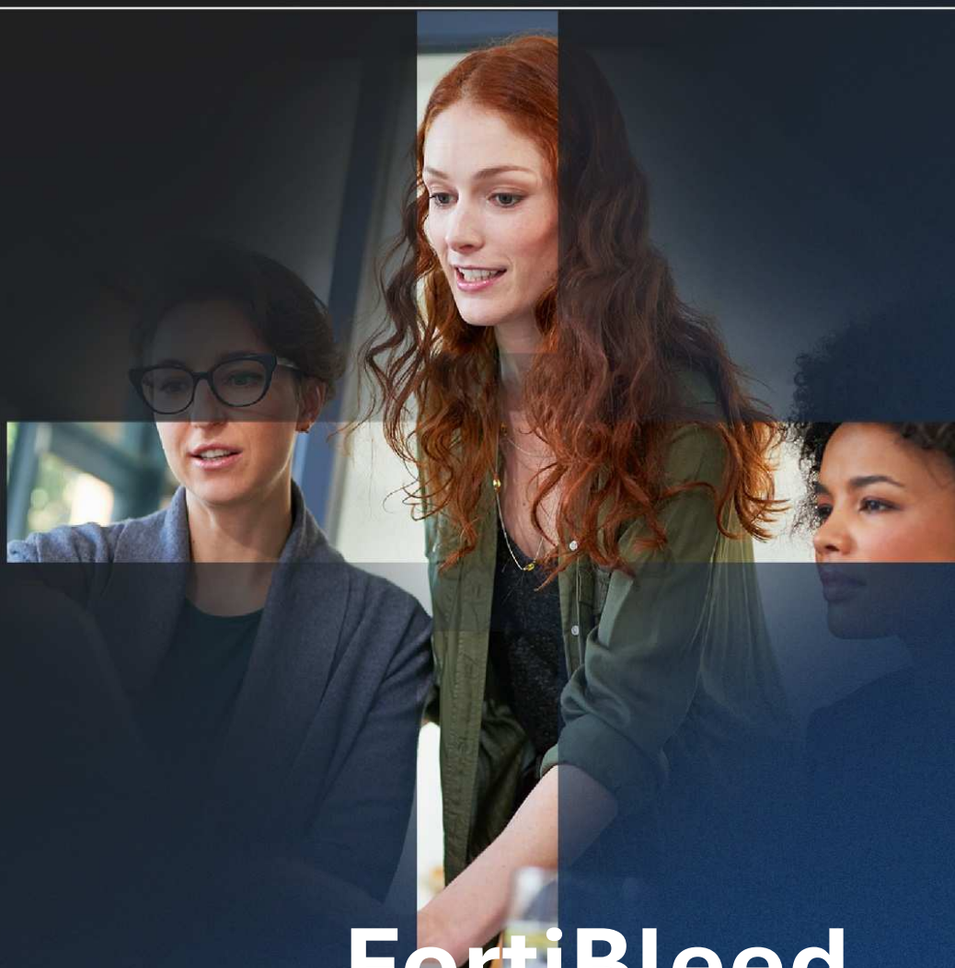
aDvens

For cyber, people & planet



FortiBleed

Compromission d’identifiants FortiGate

ADVENS
CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

SOMMAIRE

FORTIBLEED : COMPROMISSION D'IDENTIFIANTS FORTIGATE

Contexte

Des chercheurs en sécurité ont récemment mis au jour l'infrastructure opérationnelle d'un groupe cybercriminel, vraisemblablement russophone. Cette infrastructure contenait une base de données structurée d'identifiants valides pour des dizaines de milliers d'équipements Fortinet FortiGate (pare-feux nouvelle génération et passerelles SSL-VPN) déployés dans des entreprises à travers le monde.

Les investigations menées ont confirmé l'authenticité des données et estimé l'étendue de la compromission à environ 75 000 équipements, soit près de 50 % de l'ensemble des FortiGate exposés sur Internet. Certaines analyses suggèrent qu'une partie des identifiants recensés pourrait être issue de données historiques et ne plus être valide à ce jour. Néanmoins, cette réserve ne diminue pas la nécessité d'évaluer l'exposition potentielle des environnements concernés.

FortiBleed n'est pas lié à une vulnérabilité zero-day. Aucun correctif logiciel spécifique n'est donc requis. Un équipement à jour reste compromis si ses identifiants sont connus des attaquants.

Méthodes d'attaque

- Scan massif d'Internet à la recherche d'équipements FortiGate exposant leur interface d'administration ou via leur portail SSL-VPN
- Credential stuffing : exploitation de listes d'identifiants issus de fuites de données antérieures et de bases infostealer
- Password spraying et force brute : 1,16 milliard de tentatives d'authentification enregistrées contre 320 777 cibles FortiGate
- Interception et craquage hors ligne des hachages d'authentification SSL-VPN à l'aide d'un cluster de 45 GPU (via l'outil Hashtopolis)

Chaîne d'attaque et impact

Une fois l'accès obtenu, les attaquants transforment l'équipement compromis en poste d'écoute passif : le trafic réseau transitant est intercepté, permettant la collecte de nouveaux identifiants en flux continu. Ce mécanisme auto-alimenté aurait permis la construction d'une base de données vérifiée, structurée par pays, secteurs et organisations ciblées.

Des cas documentés font état de pivots vers les environnements Active Directory internes, d'exfiltration de documents sensibles dont des documents classifiés dans le cas d'un sous-traitant de l'OTAN en Turquie et de compromissions opérationnelles au-delà du seul périmètre réseau.

Secteurs et organisations concernés

La base de données FortiBleed couvre 21 632 domaines d'entreprise dans 194 pays. L'Inde et les États-Unis concentrent près d'un tiers des compromissions. Parmi les victimes figurent des multinationales telles que Foxconn, Samsung, Siemens, Lenovo, Oracle, PwC, Accenture, Comcast, AT&T, Mercedes-Benz et Toyota. Les secteurs les plus représentés incluent :

- Télécommunications : plus de 5 600 équipements compromis
- Secteur public et agences gouvernementales : 591 systèmes identifiés
- Santé, enseignement supérieur et infrastructures critiques

Recommandations

Vérifier les domaines si ils figurent dans la base FortiBleed via les outils gratuits mis à disposition par Hudson Rock (hudsonrock.com) et SOCRadar (socradar.io/blog/socradar-free-FortiBleed-exposure-checker). Une présence dans la base implique une priorité maximale sur les actions ci-dessous.

Actions prioritaires

- **Rotation immédiate des mots de passe** : Modifier l'ensemble des mots de passe des comptes administrateurs et des utilisateurs VPN sur tous les équipements FortiGate.
- **Activation du MFA** : Déployer l'authentification multifacteur (MFA) sur l'intégralité des accès administratifs et des connexions VPN.
- **Reconnexion administrative post-mise à jour** : Après toute mise à jour de FortiOS, forcer la reconnexion de chaque administrateur. Cette action active le chiffrement PBKDF2 et protège les hachages stockés contre le craquage hors ligne.
- **Restriction de l'exposition Internet**: Restreindre l'accès aux interfaces d'administration FortiGate depuis Internet (réserver l'accès au réseau interne ou à un réseau d'administration dédié). Désactiver le SSL-VPN si cette fonctionnalité n'est pas indispensable.

Actions complémentaires

- Analyser les journaux d'authentification des dernières semaines à la recherche de connexions suspectes, d'horaires inhabituels ou de sources géographiques anormales
- Auditer les comptes présents sur les équipements : détecter toute création ou modification de compte non autorisée
- Rechercher des mécanismes de persistance sur les systèmes critiques connectés (portes dérobées, tâches planifiées, scripts)
- Mettre à jour FortiOS vers la dernière version supportée et maintenir les équipements à jour en continu
- Vérifier l'intégrité des configurations FortiGate et comparer avec la dernière sauvegarde connue valide
- Étendre la surveillance aux serveurs MSSQL exposés : des tentatives de force brute parallèles ont été documentées (2,1 milliards de tentatives sur 163 650 cibles)

Conclusion

FortiBleed illustre une tendance majeure dans le paysage des menaces : la compromission par identifiants demeure le vecteur d'attaque le plus redoutable contre les infrastructures exposées sur Internet, indépendamment du niveau de mise à jour logicielle des équipements.

La mise à l'échelle industrielle de cette campagne (1,16 milliard de tentatives automatisées, craquage GPU massif, base de données structurée de victimes), confirme que les groupes cybercriminels organisés disposent désormais de capacités offensives comparables à celles d'acteurs étatiques.

La protection des accès, l'authentification forte et la surveillance continue des équipements périmétriques constituent les lignes de défense essentielles. FortiBleed rappelle que la sécurité d'un pare-feu ne se limite pas à ses correctifs logiciels : elle repose avant tout sur la robustesse et l'unicité des identifiants qui en contrôlent l'accès.

RÉFÉRENCES

- https://www.cisa.gov/news-events/alerts/2026/06/18/cisa-urges-hardening-fortinet-devices-after-reports-credential-exposure
- https://socradar.io/blog/fortibleed-fortinet-firewalls-compromised
- https://socradar.io/blog/socradar-free-fortibleed-exposure-checker
- https://www.hudsonrock.com/blog/fortibleed-75000-fortinet-firewalls-compromised-global-enterprises-exposed-claim-your-ethical-disclosure
- https://doublepulsar.com/fortibleed-75k-fortinet-firewalls-have-admin-passwords-cracked-60299faa65f8
- https://arcticwolf.com/resources/blog/active-fortibleed-campaign-impacting-fortinet-devices-across-194-countries
- https://support.huntress.io/hc/en-us/articles/52698652545171-2026-June-Fortibleed-Credential-Exposure
- https://www.securityweek.com/3-recently-patched-fortinet-fortisandbox-vulnerabilities-in-hacker-crosshairs
- https://techcrunch.com/2026/06/17/cybercriminals-allegedly-hacked-tens-of-thousands-of-fortinet-firewalls-used-by-major-companies-all-over-the-world