Systèmes opérationnels +41 21 552 03 25

DigitalCanion® Connecting Intelligent IT Services

☰

FR EN

SECURITY RESEARCH

La recherche de vulnérabilités par notre équipe de sécurité.

Nos chercheurs découvrent des failles 0-day dans les produits des plus grands éditeurs et équipementiers mondiaux : SonicWall, VMware, Sophos, Novell, Apple, Mitel, OPNsense, WatchGuard, Kyocera, Koozali : validées par la Zero Day Initiative et publiées au registre mondial CVE.



Au-delà des audits clients, notre équipe de recherche traque des vulnérabilités inédites (0-day) dans les produits des plus grands éditeurs et équipementiers mondiaux, puis les signale selon les règles de la divulgation coordonnée.

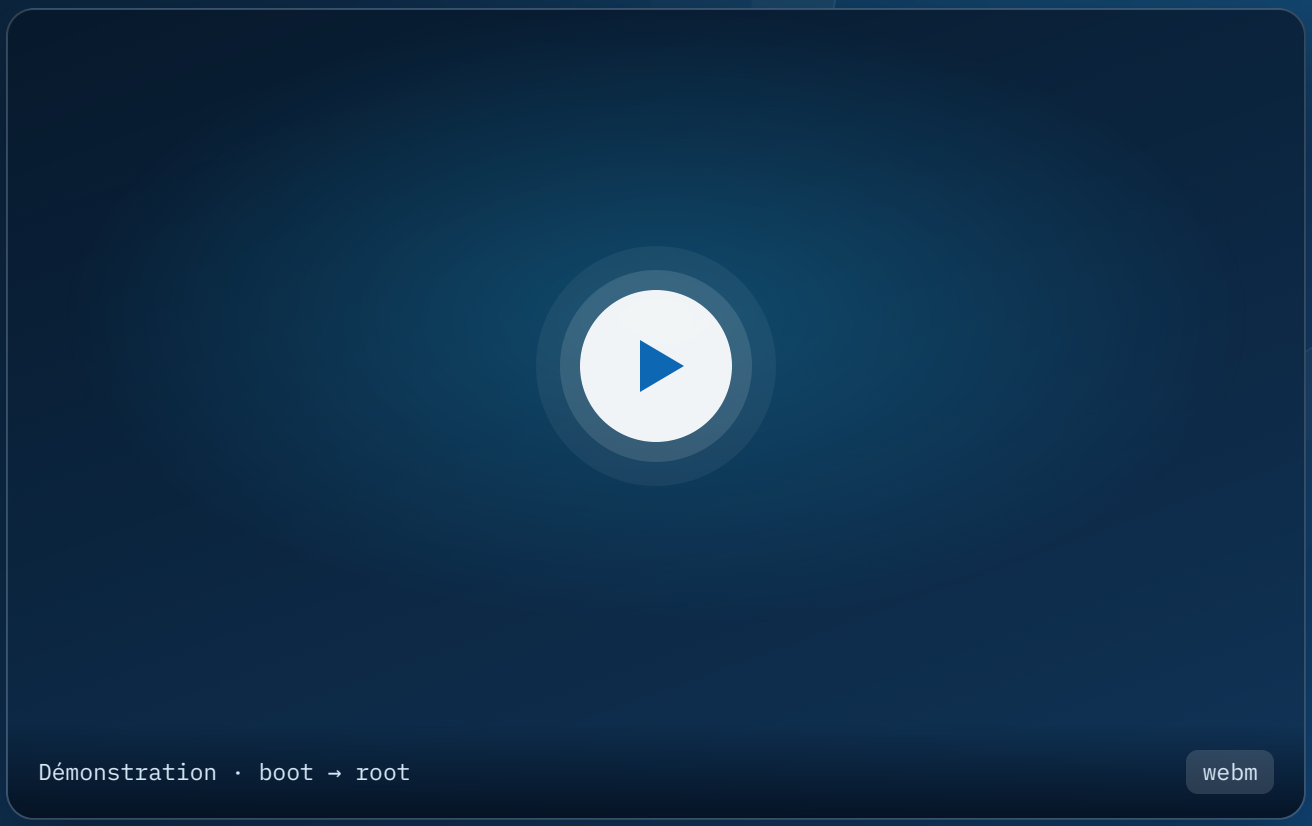
28
recherches publiées

5
advisories 0-day

27
CVE référencées

10
éditeurs

NOUVEAU PAPERS · PUBLICATIONS TECHNIQUES



Mitel MiVoice Office 400 : hijacking de bibliothèque partagée jusqu'à l'exécution de code root

Analyse technique complète et reconstruction au runtime d'une bibliothèque partagée ELF 32 bits dans l'environnement MSRV : du reverse engineering statique jusqu'à une preuve de compromission validée, vidéo à l'appui.

CVE-2026-104809 | CVSS 8.4 · High | ELF32 / i386 | Vidéo de compromission | Paper en anglais

Lire le paper → | ▶ Voir la vidéo

NOS DÉCOUVERTES

Toutes nos recherches de vulnérabilités

Chaque carte résume une découverte : éditeur, statut de divulgation, sévérité CVSS, identifiants et liens vers les sources officielles. Sélectionnez un ou plusieurs constructeurs et statuts, puis dépliez une carte pour le détail.

FILTRER LES DÉCOUVERTES — 32 résultats — Réinitialiser

CONSTRUCTEUR

SonicWall 10 | Mitel 11 | Sophos 2 | VMware 1 | OPNsense 1 | WatchGuard 2 | Kyocera 1 | Koozali 2 | Novell 1 | Apple 1

STATUT

CVE publiée 19 | CVE attribuée · NCSC 2 | À venir 4 | 0-day · non corrigé 2 | Chaîne d'exploit 2 | Démonstration 2 | Reconnu par l'éditeur 1

Combinez librement : plusieurs constructeurs, plusieurs statuts.

SONICWALL — Advisory DigitalCanion

Privilege Escalation to root access via OS Command Injection in SonicWALL Network Security Manager 4.2.0-0006-R293

Advisory DigitalCanion 2026-10-21

Démonstration vidéo

Un administrateur authentifié du SonicWALL Network Security Manager peut exploiter une vulnérabilité d'injection de commande dans le système d'exploitation pour exécuter des commandes arbitraires du système d'exploitation avec des privilèges root. Bien que le produit limite intentionnellement l'accès au...

Détails ▾

Lien direct

Voir la vidéo de démonstration →

WATCHGUARD

À venir

WatchGuard : vulnérabilité de sévérité élevée

DGI-SWISS-00037 · CVE-2026-108152

8.5 CVSS · Élevée

DigitalCanion SA a identifié une vulnérabilité de sévérité élevée dans un produit WatchGuard, évaluée CVSS 8.5 (High). Référencée DGI-SWISS-00037, elle a été signalée à l'éditeur et a déjà reçu l'identifiant CVE-2026-108152 (fiche réservée) ; la divulgation coordonnée est en cours. Les détails techniques seront...

Détails ▾

Lien direct

cve.org

KOOZALI

CVE attribuée · NCSC

Koozali SME Server : vulnérabilité de sévérité élevée

DGI-SWISS-00036 · CVE-2026-108120 2026-10-10

7.0 CVSS · Élevée

DigitalCanion SA a découvert une vulnérabilité de traversée de chemin sur Koozali SME Server v11.0.0-267.el8 dans la fonctionnalité « Afficher les journaux » du portail de gestion web. Cette vulnérabilité résulte d'une validation incorrecte des chemins d'accès aux fichiers fournis par l'utilisateur, ce qui permet à un...

Détails ▾

Lien direct

Rapport Koozali Bugzilla #13721 | cve.org | Liste CVE du NCSC

KOOZALI

CVE attribuée · NCSC

Koozali SME Server : vulnérabilité de sévérité moyenne

DGI-SWISS-00035 · CVE-2026-108121 2026-10-10

6.5 CVSS · Moyenne

DigitalCanion SA a découvert une vulnérabilité dans la fonctionnalité de création de domaines de Koozali SME Server, version 11.0rc1-215. Cette vulnérabilité résulte d'une validation insuffisante des données fournies par l'utilisateur avant leur insertion dans la configuration du serveur HTTP Apache. Un attaquant...

Détails ▾

Lien direct

cve.org | Liste CVE du NCSC

SONICWALL

CVE publiée

SonicWall SMA1000 : Zip Slip dans la console AMC menant à l'exécution de code

ZDI-CAN-28924 · CVE-2026-102257 · ZDI-26-770 · SNWLID-2026-0017 2026-10-06

7.2 CVSS · Élevée

DigitalCanion SA a identifié une vulnérabilité de type Zip Slip (traversée de répertoire à l'extraction d'archives, CWE-22) dans l'Appliance Management Console (AMC) des SonicWall SMA1000. Un administrateur authentifié peut, au moyen d'une archive spécialement conçue, écrire des fichiers en...

Détails ▾

Lien direct

Advisory ZDI ZDI-26-770 | Advisory SonicWall SNWLID-2026-0017 | cve.org | NVD | Rapid7

CERT-FR

SONICWALL

CVE publiée

SonicWall SMA1000 : Cross-Site Scripting stocké dans la console AMC

CVE-2026-102258 · SNWLID-2026-0017 2026-10-06

5.5 CVSS · Moyenne

DigitalCanion SA a identifié une vulnérabilité de Cross-Site Scripting stocké (CWE-79) dans l'Appliance Management Console (AMC) des SonicWall SMA1000. Un attaquant distant authentifié en tant qu'administrateur peut, dans certaines conditions, stocker puis faire exécuter du code JavaScript arbitrair...

Détails ▾

Lien direct

Advisory SonicWall SNWLID-2026-0017 | cve.org | NVD | Rapid7 | CERT-FR

MITEL

CVE publiée

Mitel MiVoice Office 400 : écriture de fichier arbitraire à la restauration de sauvegarde, exécution de code root

DGI-SWISS-00033 · CVE-2026-104805 2026-10-05

8.5 CVSS 4.0 · Élevée

Le mécanisme de restauration de sauvegarde de Mitel MiVoice Office 400 ne valide ni les chemins, ni les types, ni l'intégrité, ni l'authenticité des fichiers contenus dans les archives TGZ. Un attaquant disposant d'un accès au dépôt de sauvegardes peut y introduire des fichiers malveillants qui sont écrits sur le...

Détails ▾

Lien direct

cve.org | NVD | Rapid7 | Liste CVE du NCSC

MITEL

CVE publiée

Mitel MiVoice Office 400 : traversée de répertoire : lecture de fichiers système via View Logs

DGI-SWISS-00025 · CVE-2026-104706 2026-10-05

8.4 CVSS 4.0 · Élevée

Une traversée de répertoire dans le portail d'administration de Mitel MiVoice Office 400 (https://<ip>:8443, menu Administration → View Logs) permet de lire des fichiers système sensibles en dehors du répertoire prévu.

Détails ▾

Lien direct

cve.org NVD Rapid7 Liste CVE du NCSC

MITEL

CVE publiée

Mitel MiVoice Office 400 : détournement d'objet partagé (.so) menant à l'exécution de code arbitraire

DGI-SWISS-00027 · CVE-2026-104809 2026-10-05

8.4 CVSS 4.0 · Élevée

Mitel MiVoice Office 400 charge des bibliothèques partagées (.so) selon un nommage prévisible et sans vérification d'intégrité. Un attaquant peut faire charger un fichier .so qu'il contrôle à la place du module légitime ; le code s'exécute avec les privilèges du processus et conduit à la compromission complète de l...

Détails ▾

Lien direct

▶ Lire le paper + vidéo cve.org NVD Rapid7 Liste CVE du NCSC

MITEL

CVE publiée

Mitel MiVoice Office 400 : traversée de répertoire dans le navigateur de fichiers (suppression de fichiers système)

DGI-SWISS-00028 · CVE-2026-104810 2026-10-05

8.4 CVSS 4.0 · Élevée

La fonction File Management du portail web de Mitel MiVoice Office 400 ne valide pas correctement les chemins : un utilisateur authentifié peut remonter l'arborescence et supprimer des fichiers critiques de l'application ou du système, provoquant un déni de service.

Détails ▾

Lien direct

cve.org NVD Rapid7 Liste CVE du NCSC

MITEL

CVE publiée

Mitel MiVoice Office 400 : exécution de code via téléversement de fichier WAV (musique d'attente)

DGI-SWISS-00029 · CVE-2026-104811 2026-10-05

8.4 CVSS 4.0 · Élevée

La fonction Music on Hold de Mitel MiVoice Office 400 valide mal les fichiers téléversés : un attaquant peut déposer un objet partagé (.so) malveillant déguisé en fichier audio WAV, ce qui conduit à l'exécution de code arbitraire et à la compromission du système.

Détails ▾

Lien direct

cve.org NVD Rapid7 Liste CVE du NCSC

MITEL

CVE publiée

Mitel MiVoice Office 400 : traversée de répertoire dans les journaux système (divulgation d'informations)

DGI-SWISS-00032 · CVE-2026-104806 2026-10-05

5.5 CVSS 4.0 · Moyenne

La fonction System Logs du portail de gestion web de Mitel MiVoice Office 400 (TCP 443) ne valide pas correctement les chemins de fichiers, ce qui permet à un attaquant de lire des fichiers situés en dehors du répertoire prévu.

Détails ▾

Lien direct

cve.org NVD Rapid7 Liste CVE du NCSC

MITEL

CVE publiée

Mitel MiVoice Office 400 : Cross-Site Scripting stocké via le champ description des domaines

DGI-SWISS-00030 · CVE-2026-104807 2026-10-05

1.9 CVSS 4.0 · Faible

Un attaquant authentifié peut injecter du JavaScript dans le champ « Description » de Configuration → Domains du portail web de Mitel MiVoice Office 400 (TCP 443). L'entrée n'est pas assainie : le script persistant s'exécute chez les autres utilisateurs (manipulation de page, injection de contenu,...

Détails ▾

Lien direct

cve.org NVD Rapid7 Liste CVE du NCSC

MITEL

CVE publiée

Mitel MiVoice Office 400 : Cross-Site Scripting stocké via le champ « Microsoft Exchange mailbox »

DGI-SWISS-00031 · CVE-2026-104808 2026-10-05

1.9 CVSS 4.0 · Faible

Un attaquant authentifié peut injecter du JavaScript dans le champ « Microsoft Exchange mailbox » de la configuration des utilisateurs de Mitel MiVoice Office 400. Le script stocké s'exécute à chaque consultation des propriétés de l'utilisateur et peut provoquer un déni de service de l'interface.

Détails ▾

Lien direct

cve.org NVD Rapid7 Liste CVE du NCSC

KYOCERA

À venir

Kyocera : vulnérabilité de sévérité élevée

DGI-SWISS-00034

7.1 CVSS · Élevée

DigitalCanion SA, via son chercheur Brian Mariani, a identifié une vulnérabilité de sévérité élevée dans un produit Kyocera, évaluée CVSS 7.1 (High). Référencée DGI-SWISS-00034, elle a été signalée à l'éditeur et fait l'objet d'une divulgation coordonnée. Les détails techniques et l'identifiant CVE seront publiés à l'issu...

Détails ▾

Lien direct

WATCHGUARD

CVE publiée

WatchGuard Fireware OS : déni de service des outils de diagnostic

DGI-SWISS-00024 · CVE-2026-18105 2026-09-29

7.1 CVSS · Élevée

DigitalCanion SA, via son chercheur Brian Mariani, a identifié une vulnérabilité de type consommation incontrôlée de ressources (CWE-400 / CWE-770) dans WatchGuard Fireware OS, le système des firewalls Firebox. Un utilisateur authentifié à faibles privilèges peut provoquer un déni de service des outils de...

Détails ▾

Lien direct

Advisory WatchGuard PSIRT CVE-2026-18105 NVD

MITEL

0-day · non corrigé

Mitel MiVoice Office 400 : absence de Secure Boot et d'intégrité

Advisory DigitalCanion · 0-day 2026-09

0-day · non corrigé par l'éditeur

Mitel est le leader du marché des communications unifiées. Mitel MiVoice Office 400 jusqu'à la version R7.2 SP1, fonctionnant sous Linux Release 11.0.96.0, n'implémente ni Secure Boot, ni UEFI Secure Boot, ni protection d'intégrité du démarrage et du système de fichiers, ni chiffrement de disque LUKS.

Détails ▾

Lien direct

Lire l'advisory complet →

MITEL

À venir

Mitel : vulnérabilité en divulgation coordonnée

DGI-SWISS-00022 2026-09-01

9.1 CVSS · Critique

Vulnérabilité critique dans un produit Mitel, évaluée CVSS 9.1. Signalée le 1er septembre 2026 et en cours de divulgation coordonnée avant publication au registre CVE. Découverte par Brian Mariani.

Détails ▾

Lien direct

MITEL

À venir

Mitel : vulnérabilité en divulgation coordonnée

DGI-SWISS-00023 2026-09-01

7.1 CVSS · Élevée

Vulnérabilité de sévérité élevée dans un produit Mitel, évaluée CVSS 7.1. Signalée le 1er septembre 2026 et en cours de divulgation coordonnée avant publication au registre CVE. Découverte par DigitalCanion SA.

Détails ▾

Lien direct

OPNSENSE

CVE publiée

OPNsense 26.7.1_1 : Cross-Site Scripting stocké et réfléchi

GHSA-9h93-hhcx-957c · CVE-2026-115425 2026-08-12

Sévérité éditeur : Low

Réduire ▴

DigitalCanion SA a identifié plusieurs vulnérabilités de type Cross-Site Scripting dans OPNsense 26.7.1_1, divulguées de manière responsable et publiées par l'éditeur dans son advisory de sécurité GitHub (GHSA-9h93-hhcx-957c, 12 août 2026). La première est une faille Cross-Site Scripting stockée (champ Description sous Interfaces → Assignments) : un attaquant peut y injecter du JavaScript qui s'exécute pour

tout utilisateur consultant la configuration d'interface, y compris les comptes root. La seconde est une faille Cross-Site Scripting réfléchie, présente dans Firewall → Log Files → Live View. Faiblesses retenues : CWE-79 (Cross-site Scripting) et CWE-116 (encodage/échappement de sortie incorrect). Sévérité : Low. Cette vulnérabilité est référencée sous CVE-2026-115425.

Lien direct

Advisory OPNsense (GitHub) | cve.org | CWE-79 | CWE-116

SONICWALL

CVE publiée

SonicWall Email Security : injection de commandes via SNMP

ZDI-CAN-29029 · CVE-2026-66150 · ZDI-26-530

2026-08-11

7.8 CVSS · Élevée

DigitalCanion SA a identifié une vulnérabilité d'injection de commandes dans SonicWall Email Security (appliances ES 5000/5050/7000/7050/9000, VMware et Hyper-V), version 10.0.35.8405 et antérieures. Un attaquant authentifié disposant d'un accès à la CLI restreinte peut injecter des commandes système...

Détails ▾

Lien direct

Advisory ZDI ZDI-26-530 | Advisory SonicWall SNWLID-2026-0012 | Product Notice SonicWall | CVE-2026-66150

SONICWALL

CVE publiée

SonicWall Email Security : injection de commandes via netmask

ZDI-CAN-29025 · CVE-2026-66149 · ZDI-26-532

2026-08-11

7.8 CVSS · Élevée

DigitalCanion SA, via son chercheur Brian Mariani, a identifié une vulnérabilité d'injection de commandes dans SonicWall Email Security (appliances ES 5000/5050/7000/7050/9000, VMware et Hyper-V), version 10.0.35.8405 et antérieures. Un attaquant authentifié disposant d'un accès à la CLI restreinte peut inject...

Détails ▾

Lien direct

Advisory ZDI ZDI-26-532 | Advisory SonicWall SNWLID-2026-0012 | Product Notice SonicWall | CVE-2026-66149

SONICWALL

0-day · non corrigé

SonicWall GMS : injection de commandes CLI (root)

ZDI-CAN-29024 · CVE-2026-66148 · ZDI-26-531 2026-08-11

7.8 CVSS · Élevée

DigitalCanion SA a identifié une vulnérabilité de sécurité affectant les produits SonicWall et l'a divulguée de manière responsable via la Zero Day Initiative (ZDI). La vulnérabilité a reçu l'identifiant ZDI-CAN-29024 et a été évaluée CVSS 7.8 (High). Le problème a été signalé le 16 avril 2026 et coordonné selon le processus...

Détails ▾

Lien direct

SONICWALL

CVE publiée

SonicWall GMS 9.5.1 : injection de commandes et Cross-Site Scripting multiples

CVE-2026-66148 · CVE-2026-66146 · SNWLID-2026-0011 2026-08-11

6.3 CVSS · Moyenne

Deux vulnérabilités découvertes et divulguées par DigitalCanion SA dans SonicWall GMS 9.5.1 et versions antérieures. CVE-2026-66148 (CVSS 6.3) : injection de commandes authentifiée permettant à un utilisateur local à faibles privilèges d'exécuter des commandes système avec les droits root, initialement...

Détails ▾

Lien direct

CVE-2026-66148 | CVE-2026-66146 | Advisory SNWLID-2026-0011

VMWARE

Reconnue par l'éditeur

VMware 17.6 (Broadcom) : vulnérabilité reconnue, non corrigée

VMware Workstation 17.6

Sans score CVSS

Vulnérabilité découverte dans la version de VMware 17.6. Bien que Broadcom ait reconnu le problème, il a indiqué ne le résoudre que « dans les prochaines versions », sans calendrier précis. Un rapport technique complet documente la découverte.

Détails ▾

Lien direct

SOPHOS

Chaîne d'exploit · non corrigé

Sophos SFOS 21.05 : SSHD trojanisé et vol d'identifiants

Sophos SFOS 21.05.0.171

Sans score CVSS

Un attaquant disposant d'un accès R/W au stockage de la VM peut altérer les binaires système. La modification du démon SSH injecte un shell arbitraire garantissant un accès distant hautement persistant qui survit aux redémarrages : malgré les messages trompeurs de validation d'intégrité. De plus, la...

Détails ▾

Lien direct

SOPHOS

Chaîne d'exploit · non corrigé

Sophos XG (SFOS 21.5) : contournement d'authentification persistant

Sophos XG · SFOS 21.5

Sans score CVSS

Bien que cette attaque nécessite un accès préalable aux disques de la machine virtuelle, cette contrainte ne saurait justifier l'absence de mécanismes de protection adaptés. En l'état, la solution de pare-feu Sophos présente des lacunes importantes en matière de fiabilité et de résilience face aux modifications...

Détails ▾

Lien direct

SONICWALL

Démonstration

SonicWall SSL VPN 10.2.2.2 : compromission complète (EOL)

SonicWall SSL VPN 10.2.2.2

Sans score CVSS

Multiples vulnérabilités critiques affectant SonicWall SSL VPN. Bien que leur exploitation nécessite un accès en lecture et en écriture au disque virtuel de la machine, cette démonstration illustre avec quelle rapidité un initié malveillant ou un attaquant ayant obtenu un tel accès peut compromettre la sécurité du...

Détails ▾

Lien direct

SONICWALL

CVE publiée

SonicWall Email Security : Cross-Site Scripting stocké, DoS et corruption de données

CVE-2026-3468 · CVE-2026-3469 · CVE-2026-3470 · SNWLID-2026-0002 2026-03-31

Sans score CVSS

Trois vulnérabilités identifiées dans la solution SonicWall Email Security (antispam), susceptibles de mettre en risque l'infrastructure de messagerie : CVE-2026-3468, CVE-2026-3469 et CVE-2026-3470. Une remédiation rapide est essentielle pour réduire l'exposition d'une couche critique de la messagerie.

Détails ▾

Lien direct

Advisory SNWLID-2026-0002

SONICWALL

CVE publiée

SonicWall Email Security : intégrité du système de fichiers et traversée de répertoire

CVE-2025-40604 · CVE-2025-40605 · SNWLID-2025-0018 2025-11-19

7.2 CVSS · Élevée

Deux vulnérabilités de sécurité identifiées et divulguées dans les produits SonicWall, signalées par les canaux appropriés et corrigées par l'éditeur. Une illustration de l'importance des tests de sécurité continus, de la transparence et de la divulgation responsable.

Détails ▾

Lien direct

CVE-2025-40604 CVE-2025-40605 Advisory 2025-0018

NOVELL

CVE publiée

Novell : CVE-2014-0610 (bug 874533)

CVE-2014-0610 · Novell bug 874533 2014

Sans score CVSS

Vulnérabilité affectant un produit Novell (référence interne éditeur : bug 874533), publiée au registre mondial sous CVE-2014-0610. Cette recherche s'inscrit dans le parcours de Brian Mariani, aujourd'hui expert cybersécurité chez DigitalCanion SA. Le détail technique complet est disponible sur les fiches de…

Détails ▾

Lien direct

Shodan CVEDB Tenable VulDB Debian Security Tracker cve.org NVD

APPLE

CVE publiée

Apple QuickTime 7.3.1 : exécution de code via le gestionnaire Flash

CVE-2007-4707 2007

Sans score CVSS

Vulnérabilité publiée par Apple dans le bulletin de sécurité QuickTime 7.3.1. Cette recherche s'inscrit dans le parcours de Brian Mariani (alors chercheur chez Syseclabs), aujourd'hui expert cybersécurité chez DigitalCanion SA.

Détails ▾

Lien direct

🍎 Bulletin de sécurité Apple (QuickTime 7.3.1) | cve.org | NVD | Shodan CVEDB | Tenable | VulDB

REGISTRE DES ADVISORIES

Registre DGI-SWISS : tous nos identifiants d'advisory

Chaque découverte reçoit un identifiant DGI-SWISS permanent. Une fois créé, il n'est jamais supprimé : son statut évolue de « À venir » (signalée à l'éditeur, divulgation coordonnée) à « CVE attribuée » puis « CVE publiée ».

ADVISORY
DGI-SWISS-00022

ÉDITEUR
Mitel

CVSS
9.1

STATUT
À venir

CVE
-

DATE
2026-09-01

ADVISORY
DGI-SWISS-00023

ÉDITEUR
Mitel

CVSS
7.1

STATUT
À venir

CVE

-

DATE

2026-09-01

ADVISORY

DGI-SWISS-00024

ÉDITEUR

WatchGuard

CVSS

7.1

STATUT

CVE publiée

CVE

CVE-2026-18105

DATE

2026-09-29

ADVISORY

DGI-SWISS-00025

ÉDITEUR

Mitel

CVSS

8.4

STATUT

CVE publiée

CVE

CVE-2026-104706

DATE

2026-10-05

ADVISORY

DGI-SWISS-00027

ÉDITEUR

Mitel

CVSS

8.4

STATUT

CVE publiée

CVE

CVE-2026-104809

DATE

2026-10-05

ADVISORY

DGI-SWISS-00028

ÉDITEUR

Mitel

CVSS

8.4

STATUT

CVE publiée

CVE

CVE-2026-104810

DATE

2026-10-05

ADVISORY

DGI-SWISS-00029

ÉDITEUR

Mitel

CVSS

8.4

STATUT

CVE publiée

CVE

CVE-2026-104811

DATE

2026-10-05

ADVISORY

DGI-SWISS-00030

ÉDITEUR

Mitel

CVSS

1.9

STATUT

CVE publiée

CVE

CVE-2026-104807

DATE

2026-10-05

ADVISORY

DGI-SWISS-00031

ÉDITEUR

Mitel

CVSS

1.9

STATUT

CVE publiée

CVE

CVE-2026-104808

DATE

2026-10-05

ADVISORY

DGI-SWISS-00032

ÉDITEUR

Mitel

CVSS

5.5

STATUT

CVE publiée

CVE

CVE-2026-104806

DATE

2026-10-05

ADVISORY

DGI-SWISS-00033

ÉDITEUR

Mitel

CVSS

8.5

STATUT

CVE publiée

CVE

CVE-2026-104805

DATE

2026-10-05

ADVISORY

DGI-SWISS-00034

ÉDITEUR

Kyocera

CVSS

7.1

STATUT

À venir

CVE

-

DATE

à confirmer

ADVISORY

DGI-SWISS-00035

ÉDITEUR

Koozali SME Server

CVSS

6.5

STATUT

CVE attribuée · NCSC

CVE

CVE-2026-108121

DATE

2026-10-10

ADVISORY

DGI-SWISS-00036

ÉDITEUR

Koozali SME Server

CVSS

7.0

STATUT

CVE attribuée · NCSC

CVE

CVE-2026-108120

DATE

2026-10-10

ADVISORY

DGI-SWISS-00037

ÉDITEUR

WatchGuard

CVSS

8.5

STATUT

À venir

CVE

CVE-2026-108152

DATE

à confirmer

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense, de la protection de la population et des sports DDPS
Office fédéral de la cybersécurité OFCS · National Cyber Security Centre NCSC

PARTENAIRE DE DIVULGATION

Nous travaillons avec le NCSC, l'autorité fédérale de numérotation CVE

Nos vulnérabilités sont enregistrées, vérifiées et publiées au registre mondial CVE en coordination avec le **Federal Department of Defence, Civil Protection and Sport DDPS, National Cyber Security Centre NCSC, Vulnerability Management** (Office fédéral de la cybersécurité OFCS, Berne), autorité de numérotation CVE (CNA) de la Confédération suisse. Le NCSC attribue les identifiants CVE à nos découvertes et assure la coordination avec les éditeurs concernés. Huit CVE Mitel MiVoice Office 400 ont ainsi été publiées le 5 octobre 2026.

Site du NCSC → **Liste des CVE du NCSC →** **Signaler une vulnérabilité au NCSC →**

ZDI

Zero Day Initiative

TREND MICRO · ZDI RESEARCHER PROGRAM

ADVISORIES ZDI-26-530 · 531 · 532 · 770

PARTENAIRE DE VALIDATION 0-DAY

Nos 0-day sont validés par la Zero Day Initiative (ZDI)

Nos découvertes 0-day chez SonicWall sont soumises à la **Zero Day Initiative de Trend Micro**, le plus grand programme mondial indépendant de récompense de vulnérabilités. ZDI reproduit et valide chaque faille, l'achète au chercheur, coordonne la divulgation avec l'éditeur puis publie

son advisory : ZDI-26-530, ZDI-26-531, ZDI-26-532 et ZDI-26-770 (CVE-2026-66148 à 66150) créditent Brian Mariani de DigitalCanion SA, et ZDI-CAN-28924 est publié sous CVE-2026-102257 (SonicWall SMA1000, advisory SNWLID-2026-0017 et advisory ZDI-26-770).

Advisories ZDI publiés → **Advisories ZDI à venir →** **Programme ZDI →**



SonicWall PSIRT

HALL OF FAME · RESPONSIBLE DISCLOSURE

DIGITALCANION SA · SECURITY RESEARCH

RECONNAISSANCE ÉDITEUR

DigitalCanion au SonicWall PSIRT Hall of Fame

SonicWall distingue dans son **PSIRT Hall of Fame** les chercheurs qui lui signalent des vulnérabilités de manière responsable. DigitalCanion SA y figure, via son chercheur Brian Mariani, pour les failles découvertes dans Email Security, GMS, SSL VPN et SMA1000 : injection de commandes, Cross-Site Scripting stocké, traversée de répertoire et déni de service, corrigées dans les advisories SNWLID-2025-0018, SNWLID-2026-0002, 0011, 0012 et 0017.

Voir le Hall of Fame SonicWall → **Advisories SonicWall PSIRT →**

ON PARLE DE NOUS

Nos découvertes dans la presse et les bases CVE

Les vulnérabilités que nous divulguons sont publiées au registre mondial CVE, créditées à notre équipe (Brian Mariani, DigitalCanion SA) et reprises par les médias spécialisés en cybersécurité.

THE HACKER NEWS

SonicWall Patches CVSS 10.0 Pre-Authentication SSRF Flaw in SMA1000 Appliances

SECURITYWEEK

SonicWall and Splunk Patch Critical Vulnerabilities

Couvre l'advisory SNWLID-2026-0017 et cite Brian Mariani de DigitalCanion SA pour CVE-2026-102257 (Zip Slip, via la Zero Day Initiative) et CVE-2026-102258 (Cross-Site Scripting stocké). 7 octobre 2026.

Lire l'article →

Les quatre vulnérabilités SMA1000 de l'advisory SNWLID-2026-0017, dont nos CVE-2026-102257 et CVE-2026-102258, corrigées aux côtés de la SSRF critique CVSS 10. 8 octobre 2026.

Lire l'article →

CERT-FR · ANSSI

Avis CERTFR-2026-AVI-1275 : multiples vulnérabilités dans SonicWall SMA1000

L'agence nationale française reprend l'advisory SonicWall et référence CVE-2026-102257 et CVE-2026-102258 (SMA1000 12.4.3 et 12.5). 7 octobre 2026.

Voir l'avis CERT-FR →

CYBERSECURITY NEWS

Critical SonicWall Vulnerability Exploited in Attacks Following Disclosure

Exploitation active de la SSRF SMA1000 deux jours après le correctif ; l'article détaille les quatre CVE, dont le Zip Slip CVE-2026-102257 et le Cross-Site Scripting CVE-2026-102258. 13 octobre 2026.

Lire l'article →

RAPID7 · VULNERABILITY DATABASE

CVE-2026-102257 : Zip Slip dans SonicWall SMA1000 AMC

Fiche Rapid7 de la vulnérabilité découverte par DigitalCanion : CVSS 7.2 (High), CWE-22, exécution de code à distance via archive spécialement conçue. 7 octobre 2026.

Voir sur Rapid7 →

NCSC · CONFÉDÉRATION SUISSE

Liste officielle des CVE publiées par le NCSC

Nos 8 CVE Mitel MiVoice Office 400 (CVE-2026-104706, 104805 à 104811) figurent en tête de la liste des CVE attribuées par l'autorité de numérotation suisse. 5 octobre 2026.

Voir la liste du NCSC →

RAPID7 · VULNERABILITY DATABASE

Fiches Rapid7 des 8 CVE Mitel découvertes par DigitalCanion

La base de vulnérabilités Rapid7 reprend chaque fiche avec le crédit « DigitalCanion has discovered… » et le score CVSS 4.0 (jusqu'à 8.5 High). 5 octobre 2026.

Voir sur Rapid7 →

SECURITYWEEK

SonicWall Patches Critical Vulnerabilities in Discontinued GMS Platform

Couvre les advisories SonicWall SNWLID-2026-0011 (GMS, nos CVE-2026-66148 et 66146) et SNWLID-2026-0012 (Email Security, nos CVE-2026-66149 et 66150). 12 août 2026.

Lire l'article →

SECURITYWEEK

SonicWall Patches High-Severity Flaws in Firewalls, Email Security Appliance

THREATINT · REGISTRE CVE

Fiches CVE créditant DigitalCanion SA

Couvre CVE-2025-40604 et CVE-2025-40605 (SonicWall Email Security). 21 novembre 2025.

Lire l'article →

Les fiches officielles CVE-2026-3468, 3469 et 3470 (SonicWall Email Security) désignent « Brian Mariani of DigitalCanion SA » comme finder.

Voir la fiche CVE →

NICOLAS COOLMAN

SonicWall · correctifs et vulnérabilités

Actualité sécurité reprenant les correctifs SonicWall, avec crédit « Brian Mariani of DigitalCanion SA ».

Lire l'article →

Parlons de votre projet.

Plus de 12 ans d'expertise suisse à votre service. Réponse sous 24h ouvrées.

Nous contacter

DigitalCanion
Connecting Intelligent IT Services

Entreprise indépendante 100% suisse, fondée en février 2014. Plus de 12 ans de services haut de gamme, sécurisés et sur mesure.

ADRESSES

Siège
Route des Avouillons 34
1196 Gland

Bureau
Champ-de-Lune 46
1470 Estavayer-le-Lac

Stockage & matériel
Rue de Montbrillant 36
1201 Genève

LIENS RAPIDES

- Nos services
- Nos solutions
- Datacenter
- A propos
- Références clients
- Témoignages
- Support technique
- Job

CONTACT

contact@digitalcanion.com
+41 21 552 03 25
Lun à Ven, 08:30 à 17:30

LinkedIn · YouTube

⬇ Support à distance TeamViewer

©2014 à 2026 DigitalCanion SA, Tous droits réservés | Marque protégée

RGPD & Confidentialité · Site développé par DigitalCanion SA