SECURITY RESEARCH

Vulnerability research by our security team.

Our researchers discover 0-day vulnerabilities in the products of the world's largest software and hardware vendors, SonicWall, VMware, Sophos, Novell, Apple, Mitel, OPNsense, WatchGuard, Kyocera, validated by the Zero Day Initiative and published in the global CVE registry.



Beyond client audits, our research team hunts for previously unknown (0-day) vulnerabilities in the products of the world's largest software and hardware vendors, then reports them under coordinated disclosure.

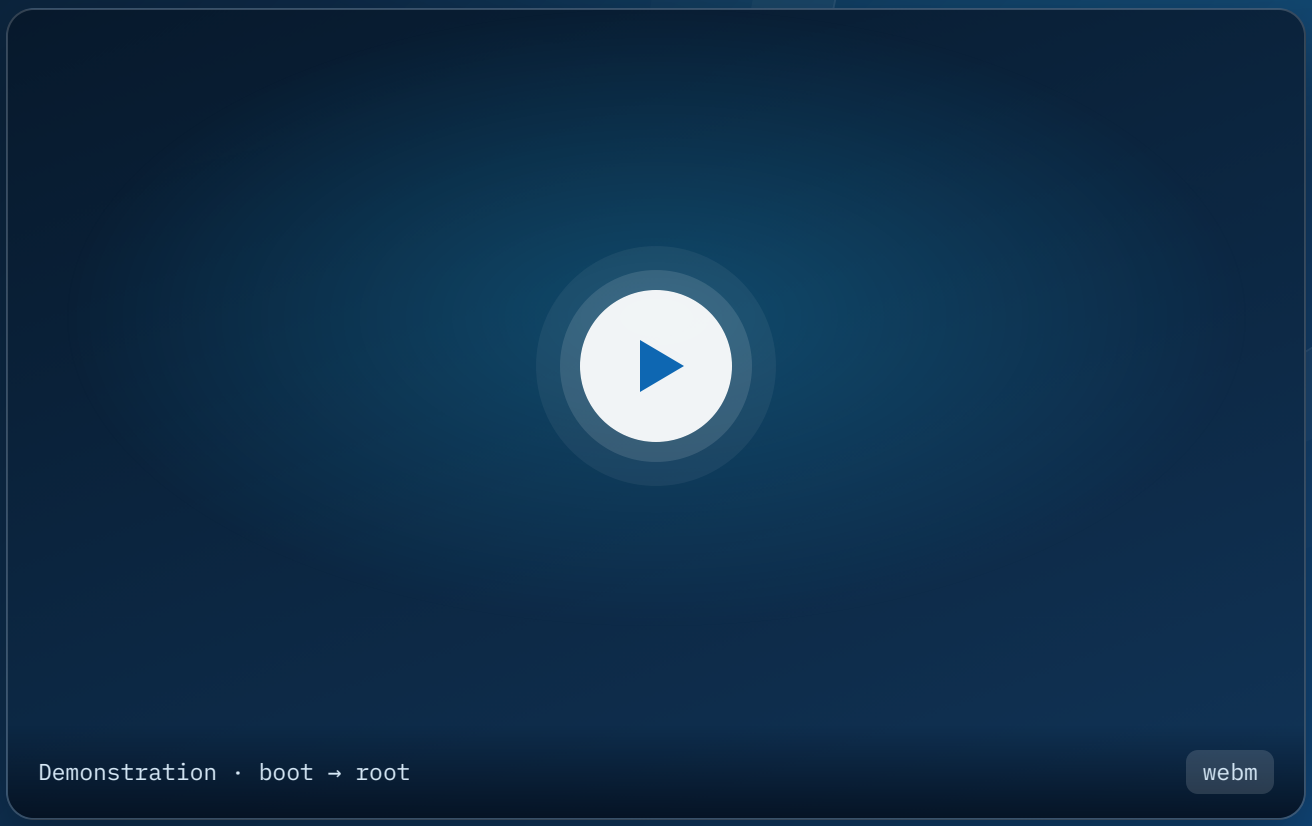
28
published findings

5
0-day advisories

27
referenced CVEs

10
vendors

NEW PAPERS · TECHNICAL PUBLICATIONS



Mitel MiVoice Office 400: shared object hijacking leading to arbitrary code execution as root

A full technical analysis and runtime reconstruction of a 32-bit ELF shared library in the MSRV environment, from static reverse engineering to a validated proof of compromise, with video.

CVE-2026-104809 | CVSS 8.4 · High | ELF32 / i386 | Proof-of-compromise video

Read the paper → | ▶ Watch the video

OUR FINDINGS

All our vulnerability research

Each card summarises one finding: vendor, disclosure status, CVSS severity, identifiers and links to official sources. Select one or more vendors and statuses, then expand a card for details.

FILTER THE FINDINGS

11 results | Reset

VENDOR

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

STATUS

Published CVE 8 | CVE assigned · NCSC 0 | Upcoming 2 | 0-day · unpatched 1 | Exploit chain 0 | Demonstration 0 | Vendor acknowledged 0

Combine freely: several vendors, several statuses.

MITEL

Published CVE

Mitel MiVoice Office 400: backup restoration arbitrary file write leading to root code execution

DGI-SWISS-00033 · CVE-2026-104805

2026-10-05

8.5 CVSS 4.0 · High

The backup restoration mechanism of Mitel MiVoice Office 400 fails to validate the paths, file types, integrity and authenticity of files contained in TGZ archives. An attacker with access to the backup repository can introduce malicious files that are written to the system during restoration, up to arbitrary...

Details ▾

Direct link

cve.org NVD Rapid7 NCSC CVE list

MITEL

Published CVE

Mitel MiVoice Office 400: path traversal: system file read via View Logs

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

8.4 CVSS 4.0 · High

A path traversal in the Mitel MiVoice Office 400 administration portal (https://<ip>:8443, Administration → View Logs menu) allows reading sensitive system files outside the intended directory.

Details ▾

Direct link

cve.org NVD Rapid7 NCSC CVE list

MITEL

Published CVE

Mitel MiVoice Office 400: shared object hijacking leading to arbitrary code execution

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

8.4 CVSS 4.0 · High

Mitel MiVoice Office 400 loads shared libraries (.so) using predictable names and without integrity verification. An attacker can make the system load an attacker-controlled .so file instead of the legitimate module; the code runs with the process privileges and leads to full compromise of the virtual machine.

Details ▾

Direct link

▶ Read the paper + video | cve.org | NVD | Rapid7 | NCSC CVE list

MITEL

Published CVE

Mitel MiVoice Office 400: file browser path traversal (deletion of system files)

DGI-SWISS-00028 · CVE-2026-104810

2026-10-05

8.4 CVSS 4.0 · High

The File Management feature of the Mitel MiVoice Office 400 web portal does not properly validate paths: an authenticated user can traverse directories and delete critical application or system files, causing a denial of service.

Details ▾

Direct link

cve.org | NVD | Rapid7 | NCSC CVE list

MITEL

Published CVE

Mitel MiVoice Office 400: code execution via WAV file upload (music on hold)

DGI-SWISS-00029 · CVE-2026-104811

2026-10-05

8.4 CVSS 4.0 · High

The Music on Hold feature of Mitel MiVoice Office 400 improperly validates uploaded files: an attacker can upload a malicious shared object (.so) disguised as a WAV audio file, leading to arbitrary code execution and system compromise.

Details ▾

Direct link

cve.org | NVD | Rapid7 | NCSC CVE list

MITEL

Published CVE

Mitel MiVoice Office 400: system logs path traversal (information disclosure)

DGI-SWISS-00032 · CVE-2026-104806

2026-10-05

5.5 CVSS 4.0 · Medium

The System Logs feature of the Mitel MiVoice Office 400 web management portal (TCP 443) fails to properly validate file paths, allowing an attacker to read files outside the intended directory.

Details ▾

Direct link

cve.org NVD Rapid7 NCSC CVE list

MITEL

Published CVE

Mitel MiVoice Office 400: stored Cross-Site Scripting via the Domains description field

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

1.9 CVSS 4.0 · Low

An authenticated attacker can inject JavaScript into the "Description" field under Configuration → Domains in the Mitel MiVoice Office 400 web portal (TCP 443). The input is not sanitised: the persistent script runs for other users (page manipulation, content injection, phishing).

Details ▾

Direct link

cve.org NVD Rapid7 NCSC CVE list

MITEL

Published CVE

Mitel MiVoice Office 400: stored Cross-Site Scripting via the "Microsoft Exchange mailbox" field

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

1.9 CVSS 4.0 · Low

An authenticated attacker can inject JavaScript into the "Microsoft Exchange mailbox" field of the Mitel MiVoice Office 400 user configuration. The stored script runs whenever the user properties are accessed and can cause a denial of service of the interface.

Details ▾

Direct link

cve.org NVD Rapid7 NCSC CVE list

MITEL

0-day · unpatched

Mitel MiVoice Office 400: no Secure Boot or integrity checks

Advisory DigitalCanion · 0-day 2026-09

0-day · unpatched by vendor

Mitel is the market leader in unified communications. Mitel MiVoice Office 400 to version R7.2 SP1, running Linux Release 11.0.96.0, does not implement Secure Boot, UEFI Secure Boot, boot/filesystem integrity protection, or LUKS disk encryption.

Details ▾

Direct link

Read the full advisory →

MITEL

Upcoming

Mitel: vulnerability under coordinated disclosure

DGI-SWISS-00022 2026-09-01

9.1 CVSS · Critical

Critical vulnerability in a Mitel product, rated CVSS 9.1. Reported on 1 September 2026 and undergoing coordinated disclosure ahead of public CVE publication. Discovered by Brian Mariani.

Details ▾

Direct link

MITEL

Upcoming

Mitel: vulnerability under coordinated disclosure

DGI-SWISS-00023 2026-09-01

7.1 CVSS · High

High-severity vulnerability in a Mitel product, rated CVSS 7.1. Reported on 1 September 2026 and undergoing coordinated disclosure ahead of public CVE publication. Discovered by DigitalCanion SA.

Details ▾

Direct link

ADVISORY REGISTRY

DGI-SWISS registry: all our advisory identifiers

Every finding receives a permanent DGI-SWISS identifier. Once created it is never removed: its status moves from "Upcoming" (reported to the vendor, coordinated disclosure) to "CVE assigned" and then "Published CVE".

ADVISORY
DGI-SWISS-00022

VENDOR
Mitel

CVSS
9.1

STATUS
Upcoming

CVE
-

DATE
2026-09-01

ADVISORY
DGI-SWISS-00023

VENDOR
Mitel

CVSS

7.1

STATUS

Upcoming

CVE

-

DATE

2026-09-01

ADVISORY

DGI-SWISS-00024

VENDOR

WatchGuard

CVSS

7.1

STATUS

Published CVE

CVE

CVE-2026-18105

DATE

2026-09-29

ADVISORY

DGI-SWISS-00025

VENDOR

Mitel

CVSS

8.4

STATUS

Published CVE

CVE

CVE-2026-104706

DATE

2026-10-05

ADVISORY

DGI-SWISS-00027

VENDOR

Mitel

CVSS

8.4

STATUS

Published CVE

CVE

CVE-2026-104809

DATE

2026-10-05

ADVISORY

DGI-SWISS-00028

VENDOR

Mitel

CVSS

8.4

STATUS

Published CVE

CVE

CVE-2026-104810

DATE

2026-10-05

ADVISORY

DGI-SWISS-00029

VENDOR

Mitel

CVSS

8.4

STATUS

Published CVE

CVE

CVE-2026-104811

DATE

2026-10-05

ADVISORY

DGI-SWISS-00030

VENDOR

Mitel

CVSS

1.9

STATUS

Published CVE

CVE

CVE-2026-104807

DATE

2026-10-05

ADVISORY

DGI-SWISS-00031

VENDOR

Mitel

CVSS

1.9

STATUS

Published CVE

CVE

CVE-2026-104808

DATE

2026-10-05

ADVISORY

DGI-SWISS-00032

VENDOR

Mitel

CVSS

5.5

STATUS

Published CVE

CVE

CVE-2026-104806

DATE

2026-10-05

ADVISORY

DGI-SWISS-00033

VENDOR

Mitel

CVSS

8.5

STATUS

Published CVE

CVE

CVE-2026-104805

DATE

2026-10-05

ADVISORY

DGI-SWISS-00034

VENDOR

Kyocera

CVSS

7.1

STATUS

Upcoming

CVE

-

DATE

to be confirmed

ADVISORY

DGI-SWISS-00035

VENDOR

Koozali SME Server

CVSS

6.5

STATUS

CVE assigned · NCSC

CVE

CVE-2026-108121

DATE

2026-10-10

ADVISORY

DGI-SWISS-00036

VENDOR

Koozali SME Server

CVSS

7.0

STATUS

CVE assigned · NCSC

CVE

CVE-2026-108120

DATE

2026-10-10

ADVISORY

DGI-SWISS-00037

VENDOR

WatchGuard

CVSS

8.5

STATUS

Upcoming

CVE

CVE-2026-108152

DATE

to be confirmed

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

DISCLOSURE PARTNER

We work with the NCSC, Switzerland's federal CVE Numbering Authority

Our vulnerabilities are registered, reviewed and published in the global CVE registry in coordination with the **Federal Department of Defence, Civil Protection and Sport DDPS, National Cyber Security Centre NCSC, Vulnerability Management** (Federal Office for Cybersecurity, Bern), the CVE Numbering Authority (CNA) of the Swiss Confederation. The NCSC assigns CVE identifiers to our findings and coordinates with the affected vendors. Eight Mitel MiVoice Office 400 CVEs were published this way on 5 October 2026.

NCSC website → **NCSC CVE list →** **Report a vulnerability to the NCSC →**

ZDI

Zero Day Initiative

TREND MICRO · ZDI RESEARCHER PROGRAM

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

0-DAY VALIDATION PARTNER

Our 0-days are validated by the Zero Day Initiative (ZDI)

Our SonicWall 0-day findings are submitted to **Trend Micro's Zero Day Initiative**, the world's largest vendor-agnostic bug bounty program. ZDI reproduces and validates each flaw, acquires it from the researcher, coordinates disclosure with the vendor and publishes its own advisory: ZDI-26-530, ZDI-26-531, ZDI-26-532 and ZDI-26-770 (CVE-2026-66148 to 66150) credit Brian Mariani of DigitalCanion SA, and ZDI-CAN-28924 was published as CVE-2026-102257 (SonicWall SMA1000, advisory SNWLID-2026-0017 and ZDI advisory ZDI-26-770).

Published ZDI advisories → **Upcoming ZDI advisories →** **ZDI program →**



SonicWall PSIRT

HALL OF FAME · RESPONSIBLE DISCLOSURE

DIGITALCANION SA · SECURITY RESEARCH

VENDOR RECOGNITION

DigitalCanion in the SonicWall PSIRT Hall of Fame

SonicWall's **PSIRT Hall of Fame** recognises researchers who report vulnerabilities to SonicWall responsibly. DigitalCanion SA is listed, through its researcher Brian Mariani, for the flaws found in Email Security, GMS, SSL VPN and SMA1000: command injection, stored Cross-Site Scripting, path traversal and denial of service, fixed in advisories SNWLID-2025-0018, SNWLID-2026-0002, 0011, 0012 and 0017.

View the SonicWall Hall of Fame → **SonicWall PSIRT advisories →**

IN THE PRESS

Our findings in the press and CVE databases

The vulnerabilities we disclose are published in the global CVE registry, credited to our team (Brian Mariani, DigitalCanion SA) and covered by specialised cybersecurity media.

THE HACKER NEWS

SECURITYWEEK

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

Covers advisory SNWLID-2026-0017 and credits Brian Mariani of DigitalCanion SA for CVE-2026-102257 (Zip Slip, via the Zero Day Initiative) and CVE-2026-102258 (stored Cross-Site Scripting). 7 October 2026.

Read the article →

SonicWall and Splunk Patch Critical Vulnerabilities

The four SMA1000 vulnerabilities of advisory SNWLID-2026-0017, including our CVE-2026-102257 and CVE-2026-102258, fixed alongside the critical CVSS 10 SSRF. 8 October 2026.

Read the article →

CERT-FR · ANSSI

Advisory CERTFR-2026-AVI-1275: multiple vulnerabilities in SonicWall SMA1000

The French national agency relays the SonicWall advisory and references CVE-2026-102257 and CVE-2026-102258 (SMA1000 12.4.3 and 12.5). 7 October 2026.

View the CERT-FR advisory →

CYBERSECURITY NEWS

Critical SonicWall Vulnerability Exploited in Attacks Following Disclosure

Active exploitation of the SMA1000 SSRF two days after the fix; the article details the four CVEs, including the Zip Slip CVE-2026-102257 and the Cross-Site Scripting CVE-2026-102258. 13 October 2026.

Read the article →

RAPID7 · VULNERABILITY DATABASE

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

Rapid7 entry for the vulnerability found by DigitalCanion: CVSS 7.2 (High), CWE-22, remote code execution via a specially crafted archive. 7 October 2026.

View on Rapid7 →

NCSC · SWISS CONFEDERATION

Official list of CVEs published by the NCSC

Our 8 Mitel MiVoice Office 400 CVEs (CVE-2026-104706, 104805 to 104811) top the list of CVEs assigned by the Swiss CVE Numbering Authority. 5 October 2026.

View the NCSC list →

RAPID7 · VULNERABILITY DATABASE

Rapid7 entries for the 8 Mitel CVEs found by DigitalCanion

The Rapid7 vulnerability database lists every record with the credit "DigitalCanion has discovered..." and the CVSS 4.0 score (up to 8.5 High). 5 October 2026.

View on Rapid7 →

SECURITYWEEK

SonicWall Patches Critical Vulnerabilities in Discontinued GMS Platform

Covers SonicWall advisories SNWLID-2026-0011 (GMS, our CVE-2026-66148 and 66146) and SNWLID-2026-0012 (Email Security, our CVE-2026-66149 and 66150). August 12, 2026.

Read the article →

SECURITYWEEK

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

Covers CVE-2025-40604 and CVE-2025-40605 (SonicWall Email Security). November 21, 2025.

Read the article →

THREATINT · CVE REGISTRY

CVE records crediting DigitalCanion SA

The official records CVE-2026-3468, 3469 and 3470 (SonicWall Email Security) name “Brian Mariani of DigitalCanion SA” as finder.

View the CVE record →

NICOLAS COOLMAN

SonicWall · patches and vulnerabilities

Security news covering the SonicWall fixes, crediting “Brian Mariani of DigitalCanion SA”.

Read the article →

Let's talk about your project.

Over 12 years of Swiss expertise at your service. Reply within 24 business hours.

Contact us

DigitalCanion
Connecting Intelligent IT Services

An independent, 100% Swiss company founded in February 2014. Over 12 years of premium, secure and tailor-made IT services.

ADDRESSES

Head office
Route des Avouillons 34
1196 Gland

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

Storage & hardware
Rue de Montbrillant 36
1201 Genève

QUICK LINKS

- Our services
- Our solutions
- Datacenter
- About us
- Client references
- Testimonials
- Technical support
- Careers

CONTACT

contact@digitalcanion.com

+41 21 552 03 25

Mon to Fri, 08:30 to 17:30

LinkedIn · YouTube

⬇ TeamViewer remote support

©2014 to 2026 DigitalCanion SA, All rights reserved | Registered trademark

GDPR & Privacy · Website developed by DigitalCanion SA