

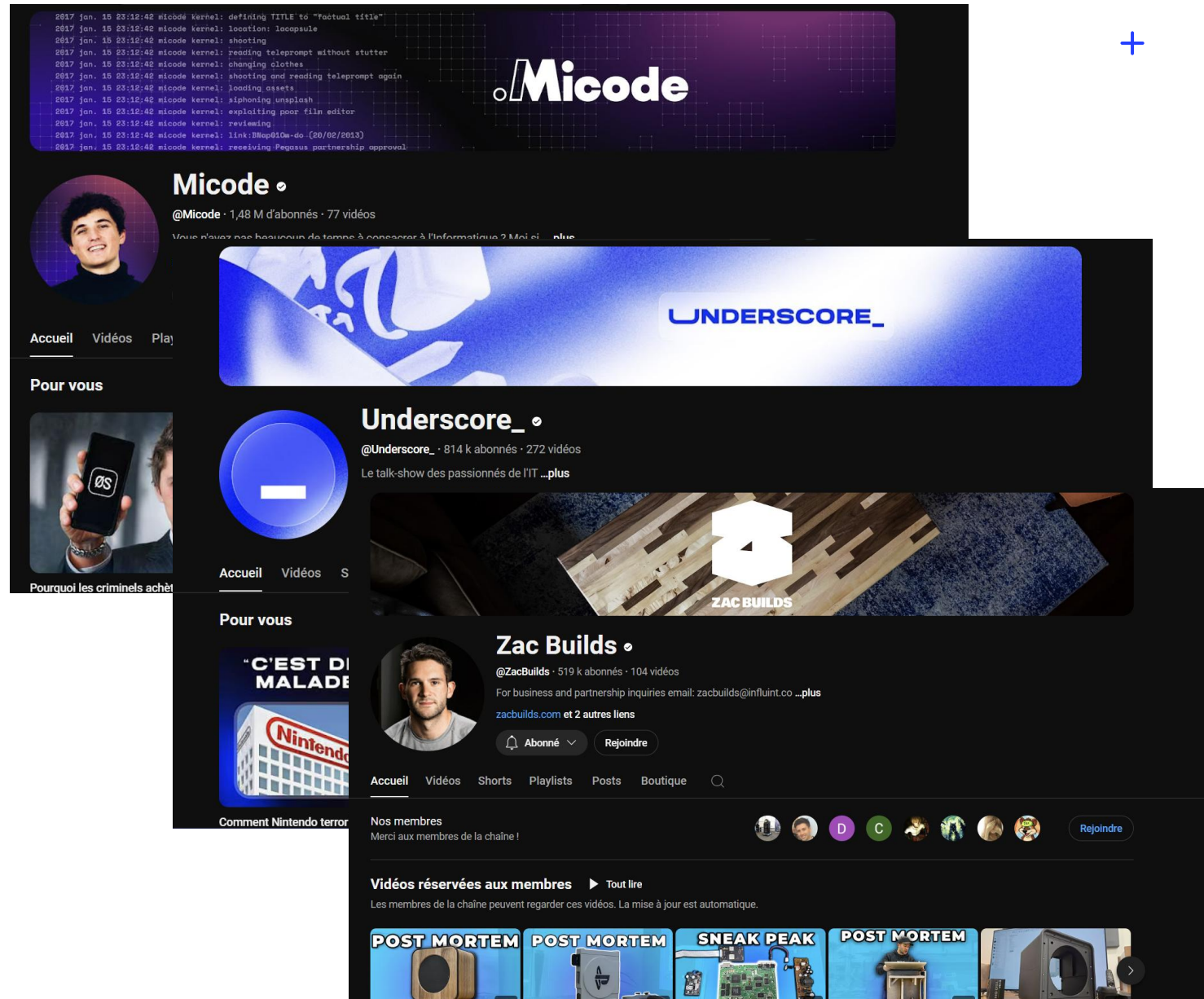
LA VEILLE TECHNOLOGIQUE



- Présenté par Jolan Noirot
- BTS SIO 2

OUTIL

- Youtube
 - Micode
 - Underscore_
 - Zac Builds



EXEMPLE

- Employer pas écouté
- Piratage en interne
- Erreur de VPN

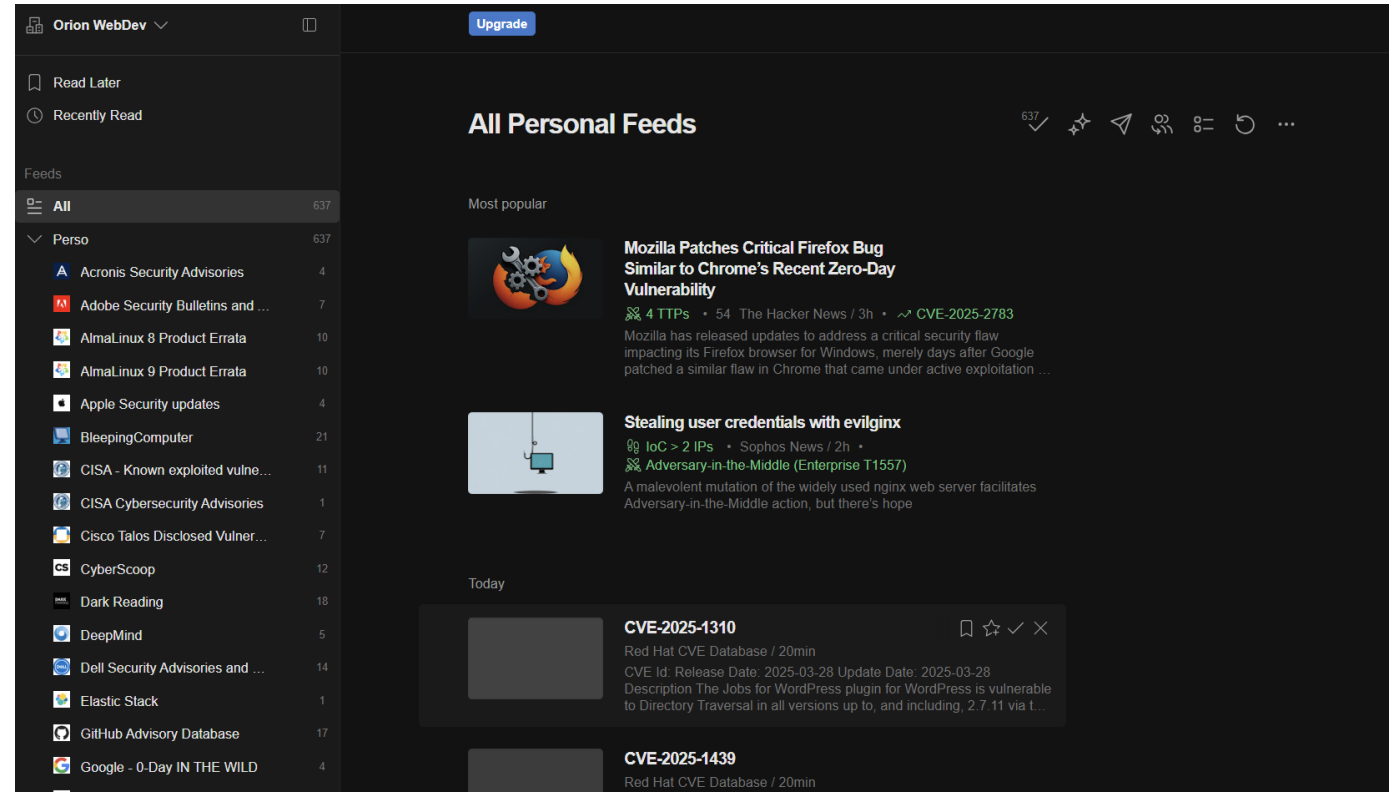


Le piratage le plus raté de l'Histoire ⋮

1,5 M de vues • il y a 8 mois

OUTIL

- Feedly
 - Cybersécurité
 - Nouvelles technologies
 - IA



EXEMPLE

- Vulnérabilité : Manipulation des réponses HTTP dans SCRIPT CASE v.1.0.002 Build7.
- Impact : Permet à un attaquant distant d'escalader ses privilèges via une requête malveillante.
- Produits affectés : Ne concerne pas les produits Red Hat, mais peut impacter d'autres systèmes utilisant SCRIPT CASE.


CVE-2025-25535

Red Hat CVE Database / Mar 28, 2025 at 2:33 AM

AI

Feedly detected 1 CVE and 1 TTP. Automatically tag, enrich, and export CVEs, Threat Actors, Malware Families, TTPs, and IoCs

[Learn More](#)

CVE Id: CVE-2025-25535 

Release Date: 2025-03-28

Update Date: 2025-03-28

Description

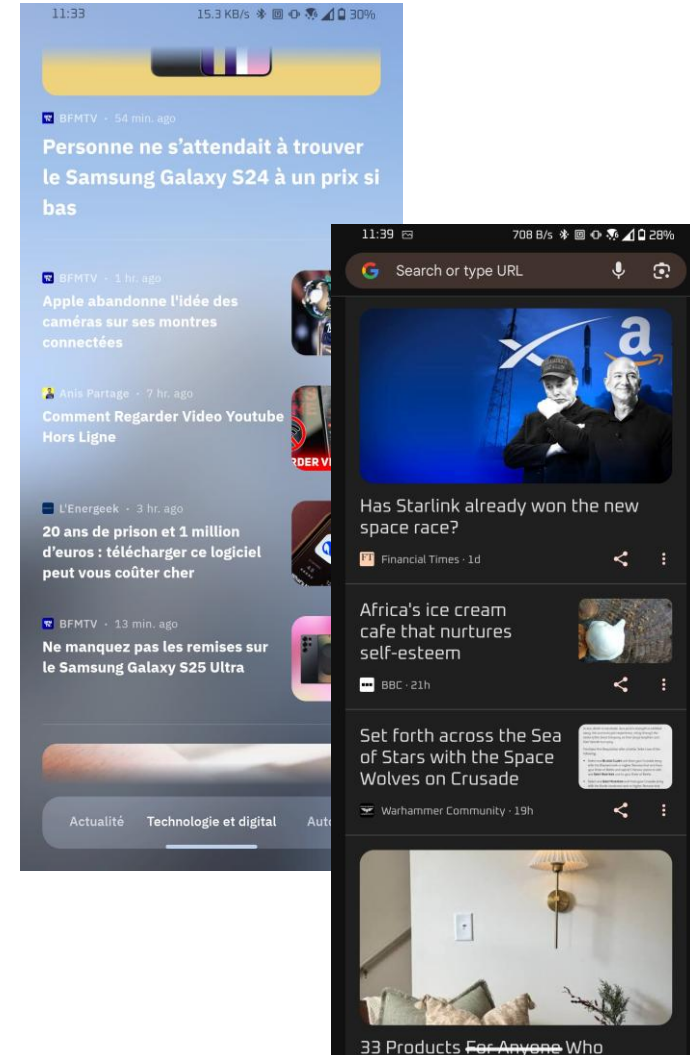
HTTP Response Manipulation in SCRIPT CASE v.1.0.002 Build7 allows a remote attacker to escalate privileges via a crafted request.

Statement

Red Hat Product Security has determined that this vulnerability does not affect

OUTIL

- **Google Discover & Microsoft Start**
 - Cybersécurité
 - Nouvelles technologies
 - IA
 - Systèmes d'exploitations



OUTIL

- OpenCVE
 - Windows
 - Ubuntu
 - Cisco
 - Fortinet

OpenCVE

Orion-WebDev

MAIN NAVIGATION

Dashboard

Projects

Orion

Manage Projects

Vulnerabilities

Vendors & Products

Weaknesses

Statistics

SETTINGS

Organizations

Tags

Profile

Admin

Logout

Orion

DashboardVulnerabilitiesReportsSubscriptionsNotifications

Activity Feed

27 mar 2025

CVE-2025-2783 has changed </>

Incorrect handle provided in unspecified circumstances in Mojo in Google Chrome on Windows prior to 134.0.6998.177 allowed a remote attacker to perform a sandbox escape via a malicious file. (Chromium security severity: High)

Metrics1 added, 0 removed

CVE-2024-27437 has changed </>

In the Linux kernel, the following vulnerability has been resolved: vfio/pci: Disable auto-enable of exclusive INTx IRQ Currently for devices requiring masking at the irqchip for INTx, ie. devices without DisINTx support, the IRQ is enabled in request_irq() and subsequently disabled as necessary to align with the masked status flag. This presents a window where the interrupt could fire between these...

First Time4 added

Weaknesses1 added, 0 removed

Cpes2 added, 0 removed

Vendors4 added, 0 removed

Metrics0 added, 0 removed

Subscriptions

Vendors (13)

Uptime Kuma ProjectUptime.kumaLinuxAndroidCiscoDockerMicrosoftJuniperRaspberrypiGooglePhpmyadminUbuntuFortinet

Products (3)

Djangoproject djangoDebian apache2Microsoft all Windows

Last Reports

Date	Number of Changes
Thu 27 Mar 2025	58
Wed 26 Mar 2025	95
Tue 25 Mar 2025	99
Mon 24 Mar 2025	119
Sun 23 Mar 2025	5
Fri 21 Mar 2025	69
Thu 20 Mar 2025	66

Jolan

EXEMPLE

Faible concernant un fichier temporaire de Remote Desktop qui permet à l'attaquant d'accéder à des informations sensibles.

[Lien vers la CVE](#)

CVE-2024-2403

Improper cleanup in temporary file handling component in Devolutions Remote Desktop Manager 2024.1.12 and earlier on Windows allows an attacker that compromised a user endpoint, under specific circumstances, to access sensitive information via residual files in the temporary directory.

Metrics



Affected Vendors & Products

All **NVD** CPE Configurations Affected Packages

Vendors	Products
Devolutions	<ul style="list-style-type: none">Remote Desktop Manager
Microsoft	<ul style="list-style-type: none">Windows

References

Link	Providers
https://devolutions.net/security/advisories/DEVO-2024-0004	CVE NVD

FIN

+

•

○