OpenCVE

« CVE Alerting Platform »

OSSIR – 11/07/2023

Bonjour

Je suis Nicolas Crocfer

@ncrocfer

/nicolascrocfer

EIFFAGE

ANSSI

OVHcloud

1.

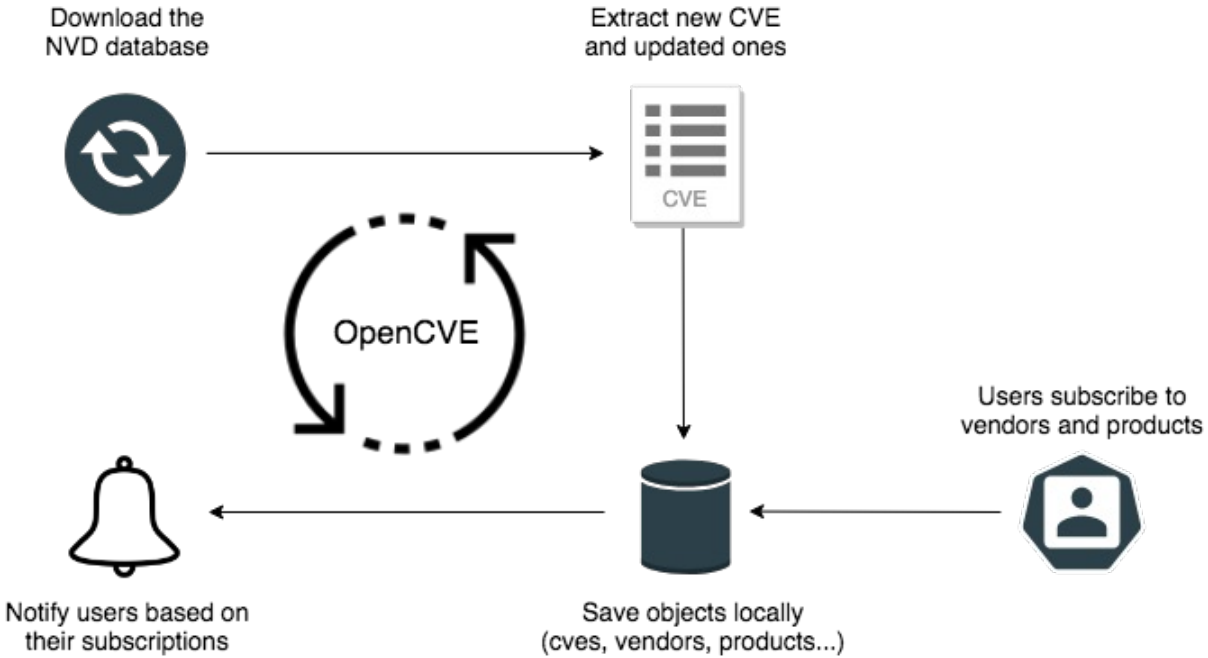
OpenCVE “v1”

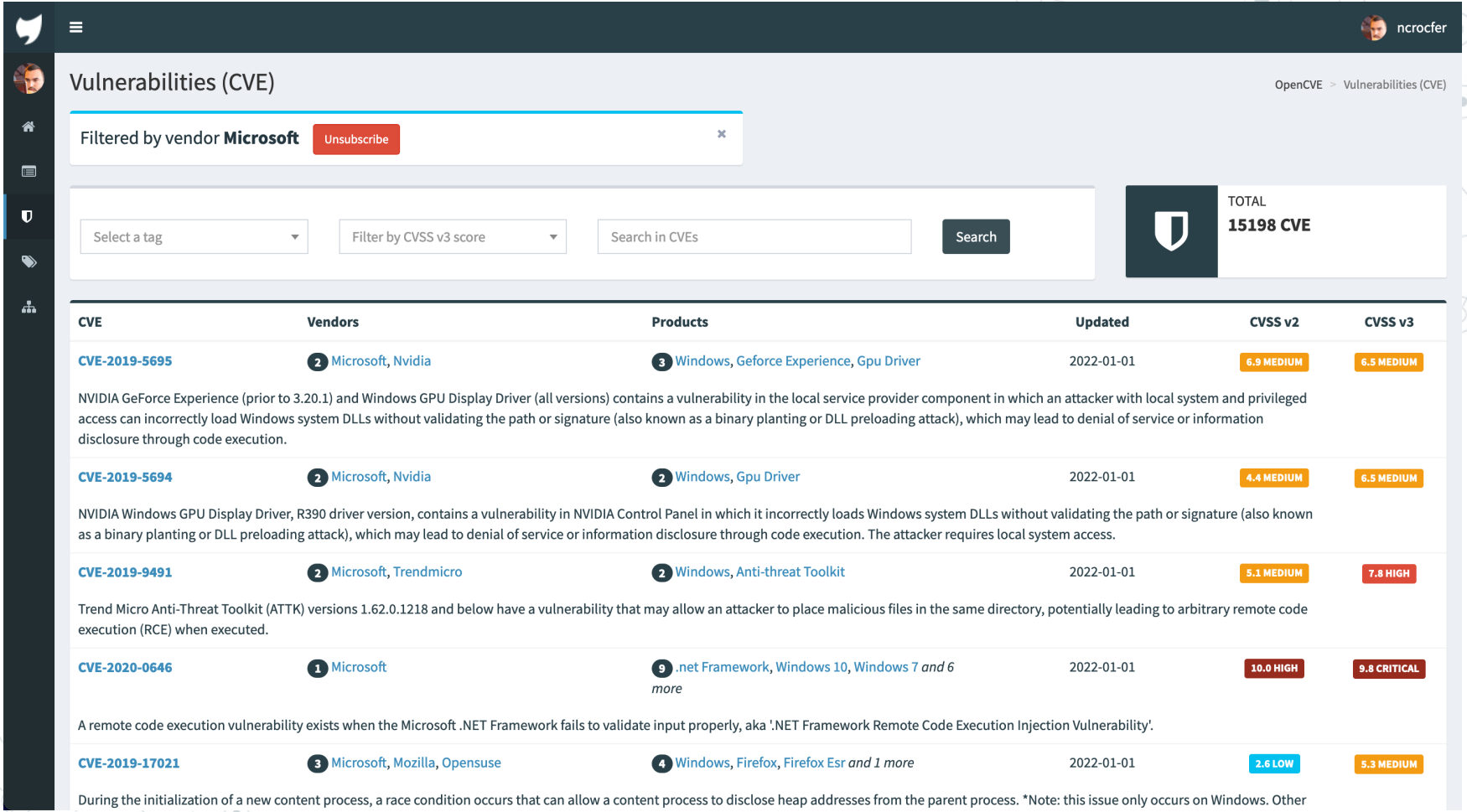
Présentation de la solution actuelle

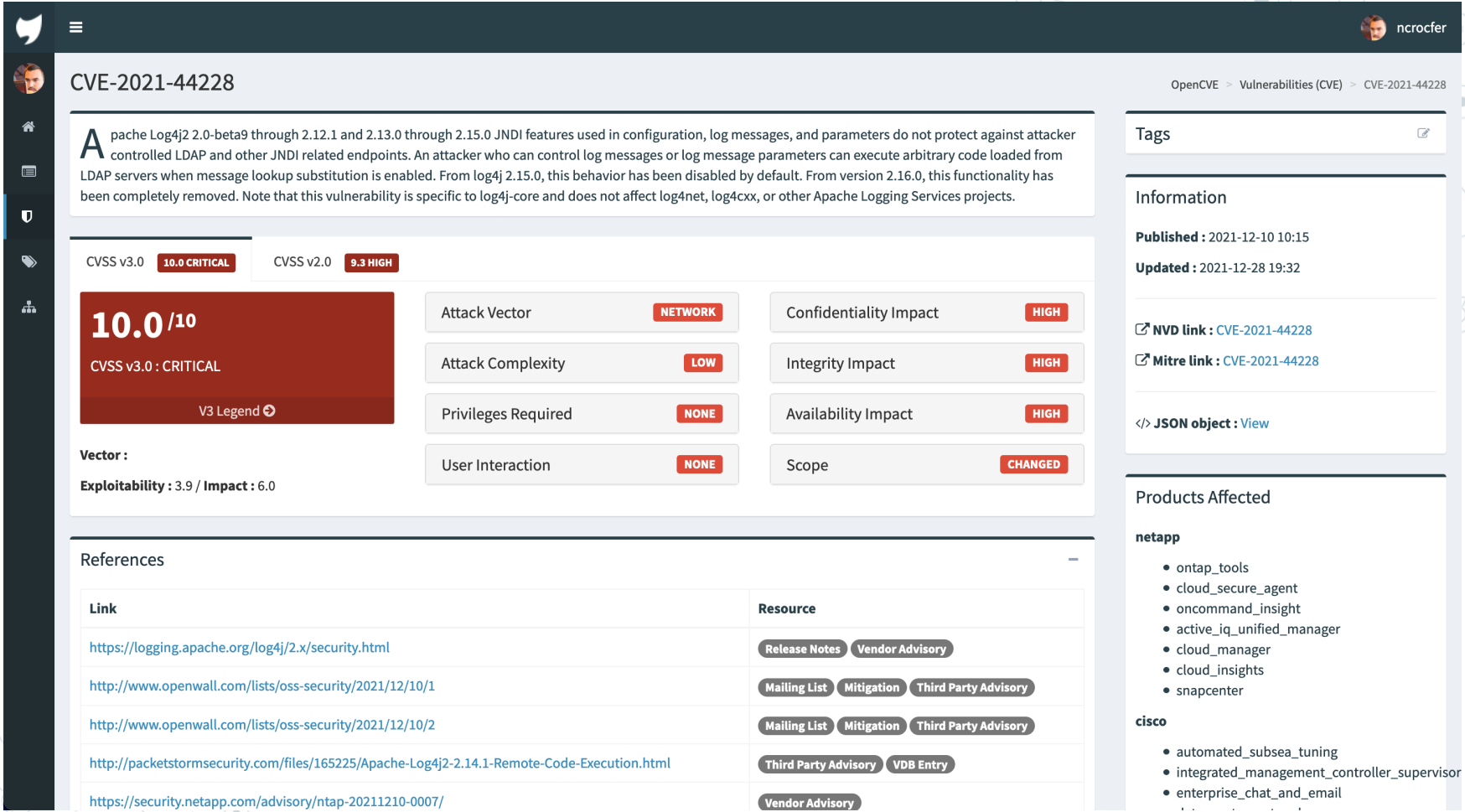
Présentation d'OpenCVE v1

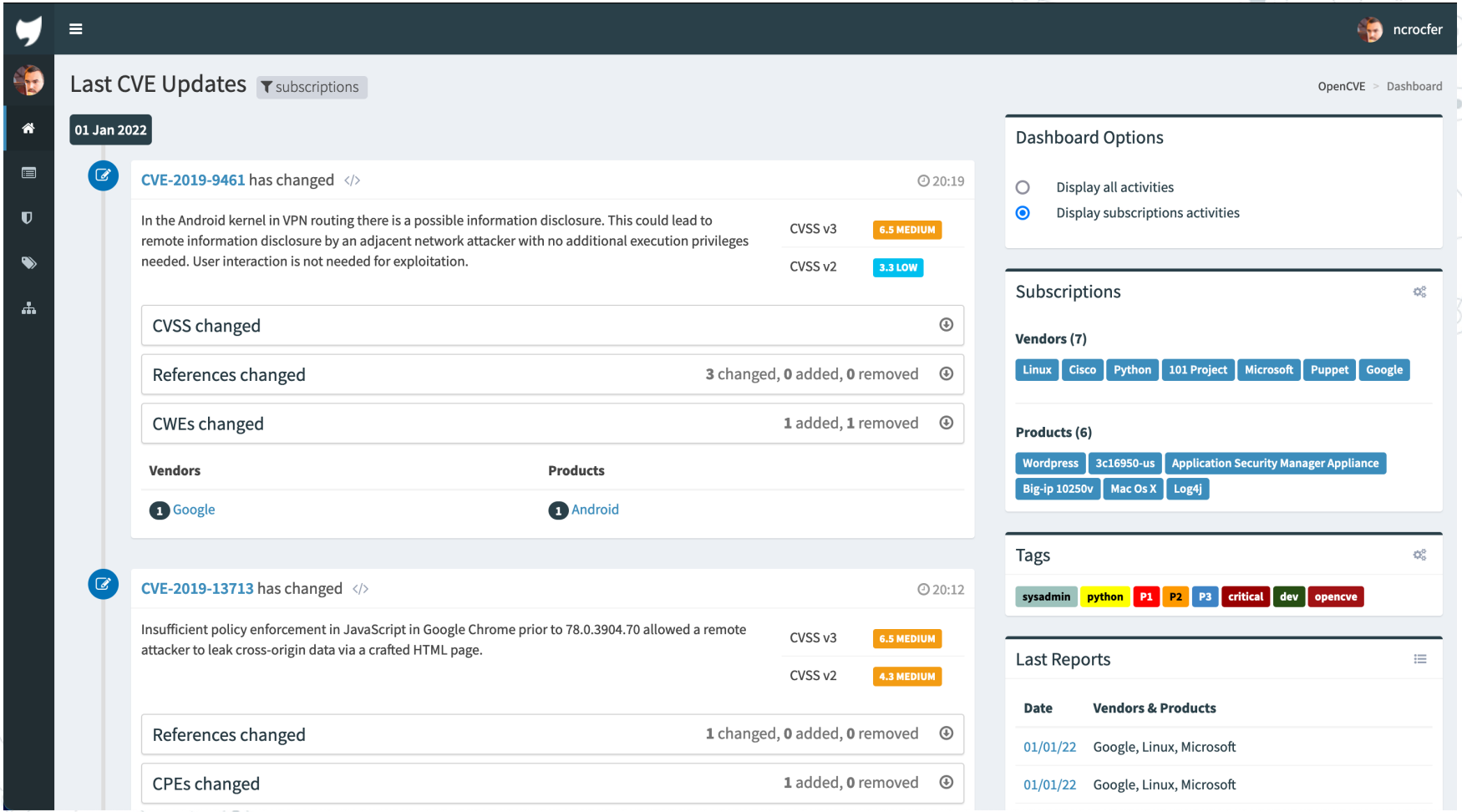
- Solution web de **vulnerability management** (*https://opencve.io*)
- **Télécharge** périodiquement les nouvelles **vulnérabilités** publiées par le NVD
- Permet d'**explorer** la base de données (par CVSS, CWE, Vendor, Product…)
- **Alerte** les utilisateurs en fonction de leurs **abonnements**

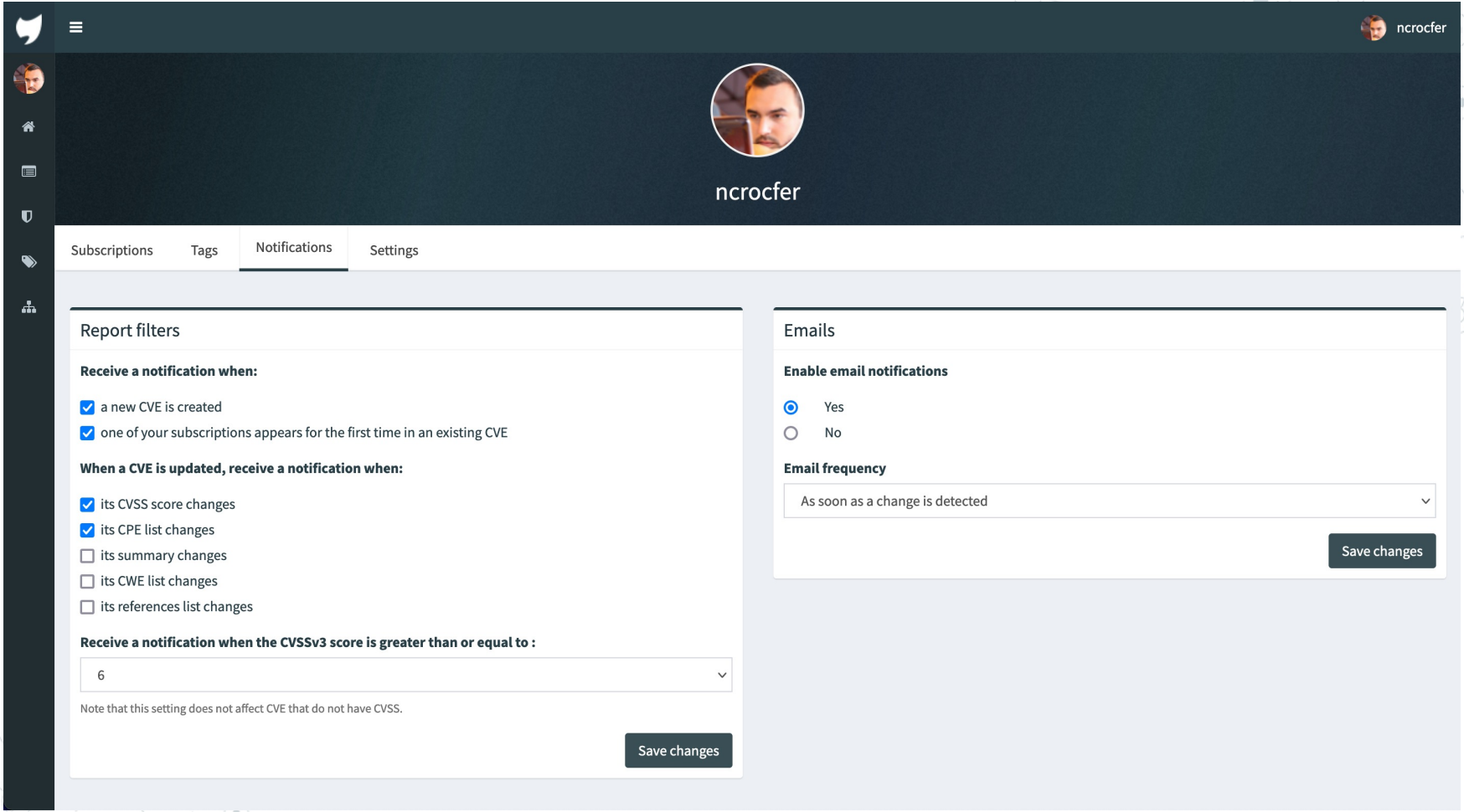
Présentation d'OpenCVE v1




ncrocfer
Vulnerabilities (CVE)
OpenCVE > Vulnerabilities (CVE)
Filtered by vendor Microsoft
Unsubscribe
Select a tag
Filter by CVSS v3 score
Search in CVEs
Search
TOTAL
15198 CVE
CVE
Vendors
Products
Updated
CVSS v2
CVSS v3
CVE-2019-5695
2 Microsoft, Nvidia
3 Windows, Geforce Experience, Gpu Driver
2022-01-01
6.9 MEDIUM
6.5 MEDIUM
NVIDIA GeForce Experience (prior to 3.20.1) and Windows GPU Display Driver (all versions) contains a vulnerability in the local service provider component in which an attacker with local system and privileged access can incorrectly load Windows system DLLs without validating the path or signature (also known as a binary planting or DLL preloading attack), which may lead to denial of service or information disclosure through code execution.
CVE-2019-5694
2 Microsoft, Nvidia
2 Windows, Gpu Driver
2022-01-01
4.4 MEDIUM
6.5 MEDIUM
NVIDIA Windows GPU Display Driver, R390 driver version, contains a vulnerability in NVIDIA Control Panel in which it incorrectly loads Windows system DLLs without validating the path or signature (also known as a binary planting or DLL preloading attack), which may lead to denial of service or information disclosure through code execution. The attacker requires local system access.
CVE-2019-9491
2 Microsoft, Trendmicro
2 Windows, Anti-threat Toolkit
2022-01-01
5.1 MEDIUM
7.8 HIGH
Trend Micro Anti-Threat Toolkit (ATTK) versions 1.62.0.1218 and below have a vulnerability that may allow an attacker to place malicious files in the same directory, potentially leading to arbitrary remote code execution (RCE) when executed.
CVE-2020-0646
1 Microsoft
9 .net Framework, Windows 10, Windows 7 and 6 more
2022-01-01
10.0 HIGH
9.8 CRITICAL
A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly, aka '.NET Framework Remote Code Execution Injection Vulnerability'.
CVE-2019-17021
3 Microsoft, Mozilla, Opensuse
4 Windows, Firefox, Firefox Esr and 1 more
2022-01-01
2.6 LOW
5.3 MEDIUM
During the initialization of a new content process, a race condition occurs that can allow a content process to disclose heap addresses from the parent process. *Note: this issue only occurs on Windows. Other


ncrocfer
CVE-2021-44228
OpenCVE > Vulnerabilities (CVE) > CVE-2021-44228
Apache Log4j2 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0, this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.
CVSS v3.0 10.0 CRITICAL
CVSS v2.0 9.3 HIGH
10.0 /10
CVSS v3.0 : CRITICAL
V3 Legend
Vector :
Exploitability : 3.9 / Impact : 6.0
Attack Vector NETWORK
Attack Complexity LOW
Privileges Required NONE
User Interaction NONE
Confidentiality Impact HIGH
Integrity Impact HIGH
Availability Impact HIGH
Scope CHANGED
References
Link
Resource
https://logging.apache.org/log4j/2.x/security.html
Release Notes Vendor Advisory
http://www.openwall.com/lists/oss-security/2021/12/10/1
Mailing List Mitigation Third Party Advisory
http://www.openwall.com/lists/oss-security/2021/12/10/2
Mailing List Mitigation Third Party Advisory
http://packetstormsecurity.com/files/165225/Apache-Log4j2-2.14.1-Remote-Code-Execution.html
Third Party Advisory VDB Entry
https://security.netapp.com/advisory/ntap-20211210-0007/
Vendor Advisory
Tags
Information
Published : 2021-12-10 10:15
Updated : 2021-12-28 19:32
NVD link : CVE-2021-44228
Mitre link : CVE-2021-44228
JSON object : View
Products Affected
netapp
ontap_tools
cloud_secure_agent
oncommand_insight
active_iq_unified_manager
cloud_manager
cloud_insights
snapcenter
cisco
automated_subsea_tuning
integrated_management_controller_supervisor
enterprise_chat_and_email


ncrocfer
Last CVE Updates
subscriptions
OpenCVE > Dashboard
01 Jan 2022
CVE-2019-9461 has changed
20:19
In the Android kernel in VPN routing there is a possible information disclosure. This could lead to remote information disclosure by an adjacent network attacker with no additional execution privileges needed. User interaction is not needed for exploitation.
CVSS v3
6.5 MEDIUM
CVSS v2
3.3 LOW
CVSS changed
References changed
3 changed, 0 added, 0 removed
CWEs changed
1 added, 1 removed
Vendors
Products
1 Google
1 Android
CVE-2019-13713 has changed
20:12
Insufficient policy enforcement in JavaScript in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVSS v3
6.5 MEDIUM
CVSS v2
4.3 MEDIUM
References changed
1 changed, 0 added, 0 removed
CPEs changed
1 added, 0 removed
Dashboard Options
Display all activities
Display subscriptions activities
Subscriptions
Vendors (7)
Linux
Cisco
Python
101 Project
Microsoft
Puppet
Google
Products (6)
Wordpress
3c16950-us
Application Security Manager Appliance
Big-ip 10250v
Mac Os X
Log4j
Tags
sysadmin
python
P1
P2
P3
critical
dev
opencve
Last Reports
Date
Vendors & Products
01/01/22
Google, Linux, Microsoft
01/01/22
Google, Linux, Microsoft


ncrocfer
ncrocfer
Subscriptions
Tags
Notifications
Settings
Report filters
Receive a notification when:
a new CVE is created
one of your subscriptions appears for the first time in an existing CVE
When a CVE is updated, receive a notification when:
its CVSS score changes
its CPE list changes
its summary changes
its CWE list changes
its references list changes
Receive a notification when the CVSSv3 score is greater than or equal to :
6
Note that this setting does not affect CVE that do not have CVSS.
Save changes
Emails
Enable email notifications
Yes
No
Email frequency
As soon as a change is detected
Save changes

4 alerts on Linux Boîte de réception ×

OpenCVE.io <no-reply@opencve.io>
À moi

mer. 5 juil. 21:15 (il y a 6 jours)

anglais › français Traduire le message Désactiver pour : anglais ×

View the full report.

Linux

CVE-2023-34460 - 9.8

Tauri is a framework for building binaries for all major desktop platforms. The 1.4.0 release includes a regression on the Filesystem scope check for dotfiles on Unix. Previously dotfiles were not implicitly allowed by the...

Changes : *CVSS changed, Vendors/Products appeared for the first time, References changed, CPEs changed*

CVE-2023-26276 - 7.5

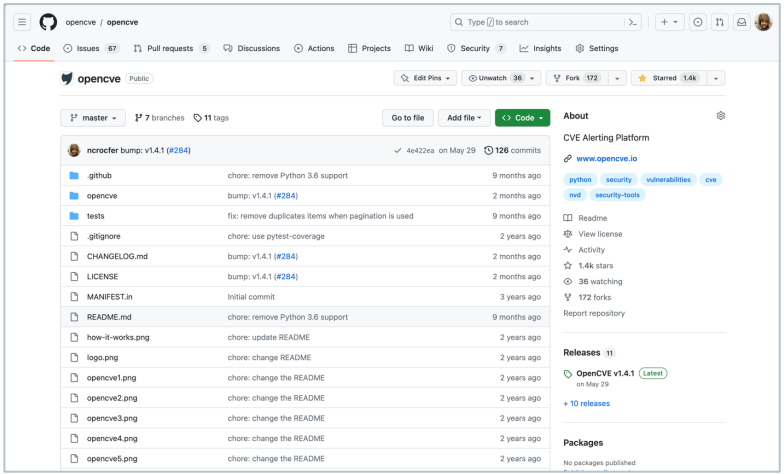
IBM QRadar SIEM 7.5.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 248147.

Changes : *References changed, CWEs changed, CVSS changed, Vendors/Products appeared for the first time, CPEs changed*

CVE-2023-3317 - 7.1

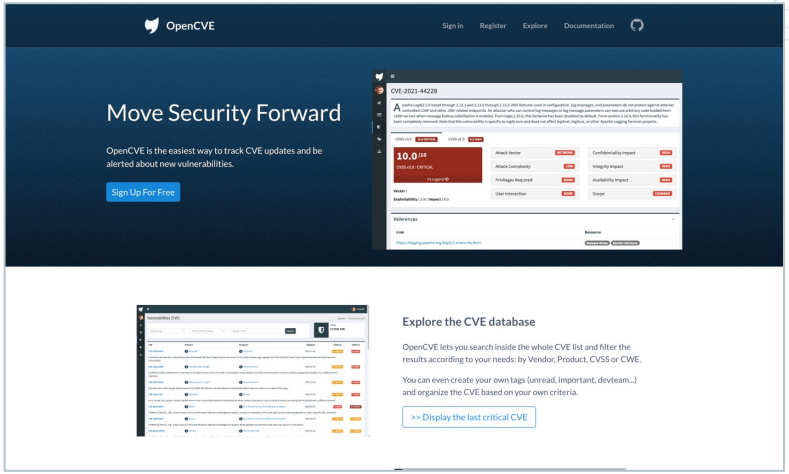
Présentation d'OpenCVE v1

Installation On-premise



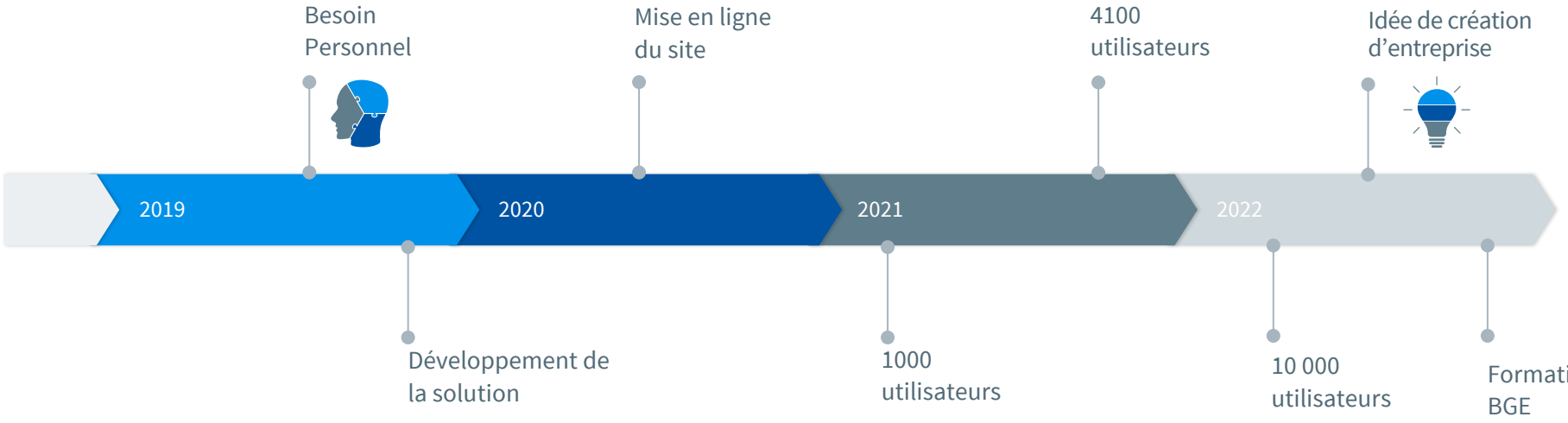
https://github.com/opencve/opencve

Instance SaaS



https://www.opencve.io/

Chronologie



18 500

utilisateurs inscrits

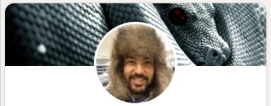
3 800 000

rapports envoyés *(+1M saucs)*

2.
Création d'entreprise

Recherche

Accueil | Réseau | Offres d'emploi | Messagerie | Notifications | Vous | Produits | Essayez Premium gratuitement



Nicolas Crocfer

IT Director chez OVHcloud

Voir le profil complet

Nicolas Crocfer • Vous

IT Director chez OVHcloud

1 mois •

Si vous me suivez vous savez que j'ai développé un outil nommé OpenCVE: https://lnkd.in/d_TbDYH

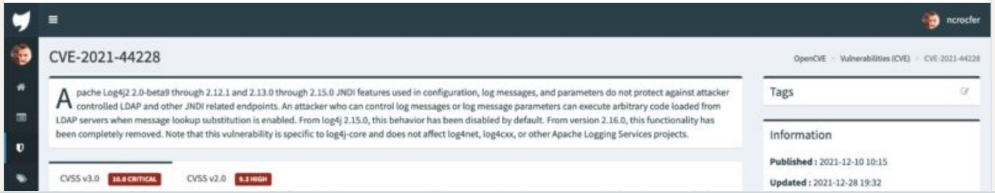
Que vous soyez RSSI, Directeur de la Cyber, Sysadmin ou simplement passionné par la sécurité informatique il se peut que vous soyez intéressé: OpenCVE vous permet de vous abonner à des produits et d'être notifié dès lors qu'une CVE apparaît.

Je travaille maintenant à l'améliorer et j'ai besoin de vous:

- pour les utilisateurs actuels quelle est la fonctionnalité manquante selon vous?
- d'un point de vue plus global, et même sans utiliser OpenCVE, qu'attendez-vous d'un outil de Vulnerability Management?
- si vous en utilisez déjà un, #cyber lequel pourriez-vous me recommander?

Merci d'avance à ceux qui me répondront à l'une ou l'autre de ces questions (ici ou en MP), ça sera très utile pour la suite de l'aventure !

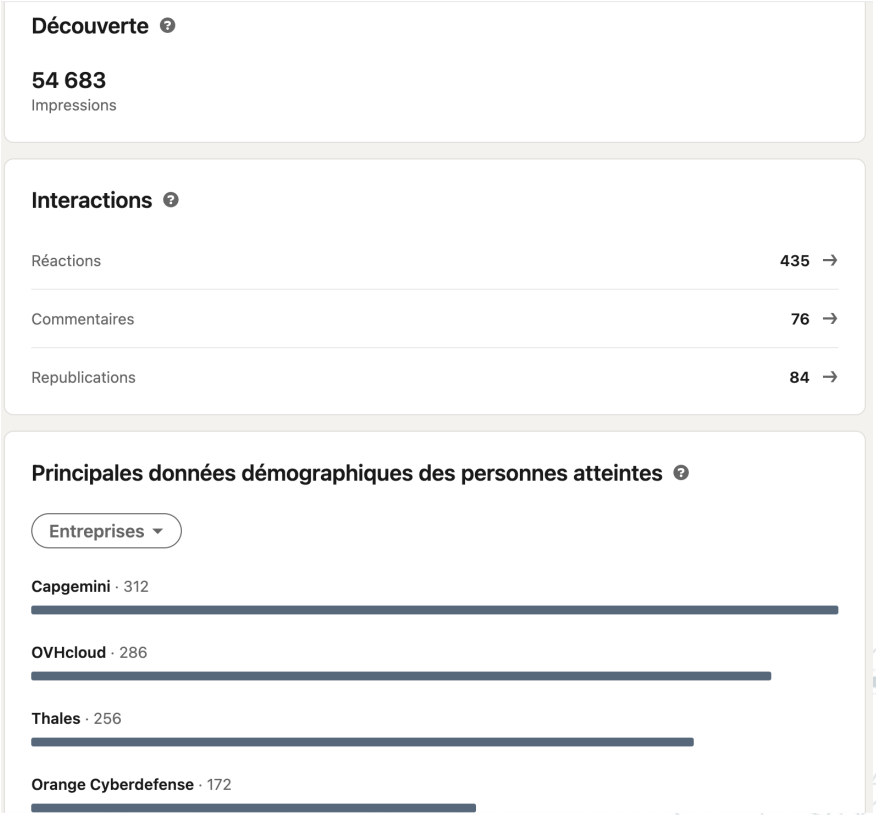
Et si vous n'utilisez pas ce genre de tool aucun soucis, c'est peut-être le cas de vos abonnés et dans ce cas n'hésitez pas à repartager cette publication 👍



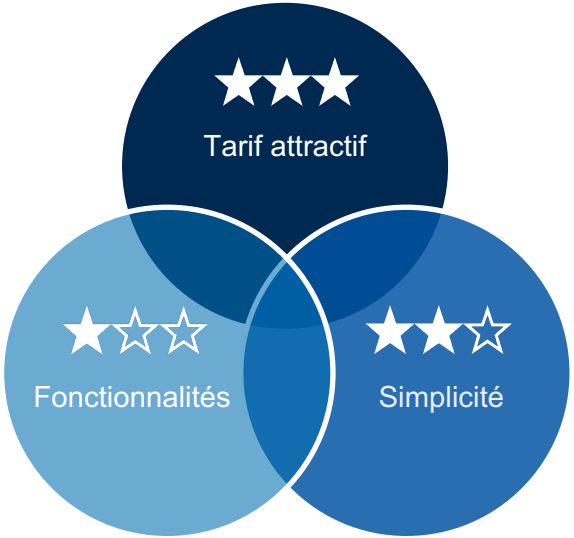
54 683
impressions

76
commentaires

84
republications



Etude de la clientèle



Carole

CEO

*« Je souhaite une solution **peu onéreuse** »*

Franck

RSSI

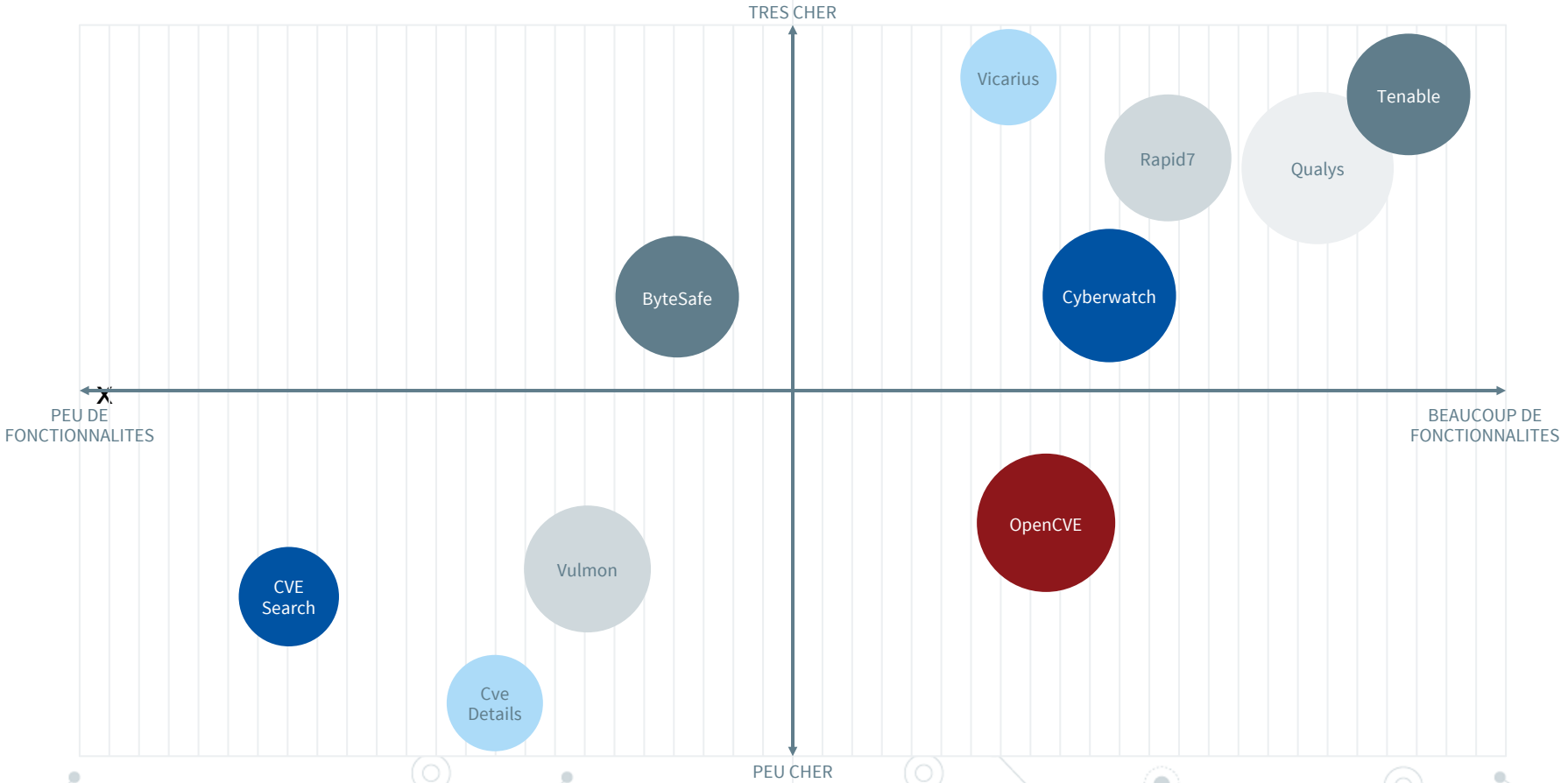
*« Je souhaite une solution **claire** et **concise** »*

Anna

ANALYSTE CYBERSECURITE

*« Je souhaite une solution **simple** et **utile** »*

Analyse de la concurrence



Création d'entreprise

- Création avec **Laurent Durnez** d'une SAS autour d'OpenCVE
- Intégration en Juin 2023 du **Campus Cyber HDF**, opéré par **Euratechnologies**

- Les 4 missions du Campus Cyber:
  - Opérer – Prévenir et réagir face aux attaques
  - Former – Sensibiliser à la cybersécurité
  - Mobiliser – Fédérer et animer l'écosystème
  - Innover - Faire émerger les champions de demain

3.
OpenCVE “v2”

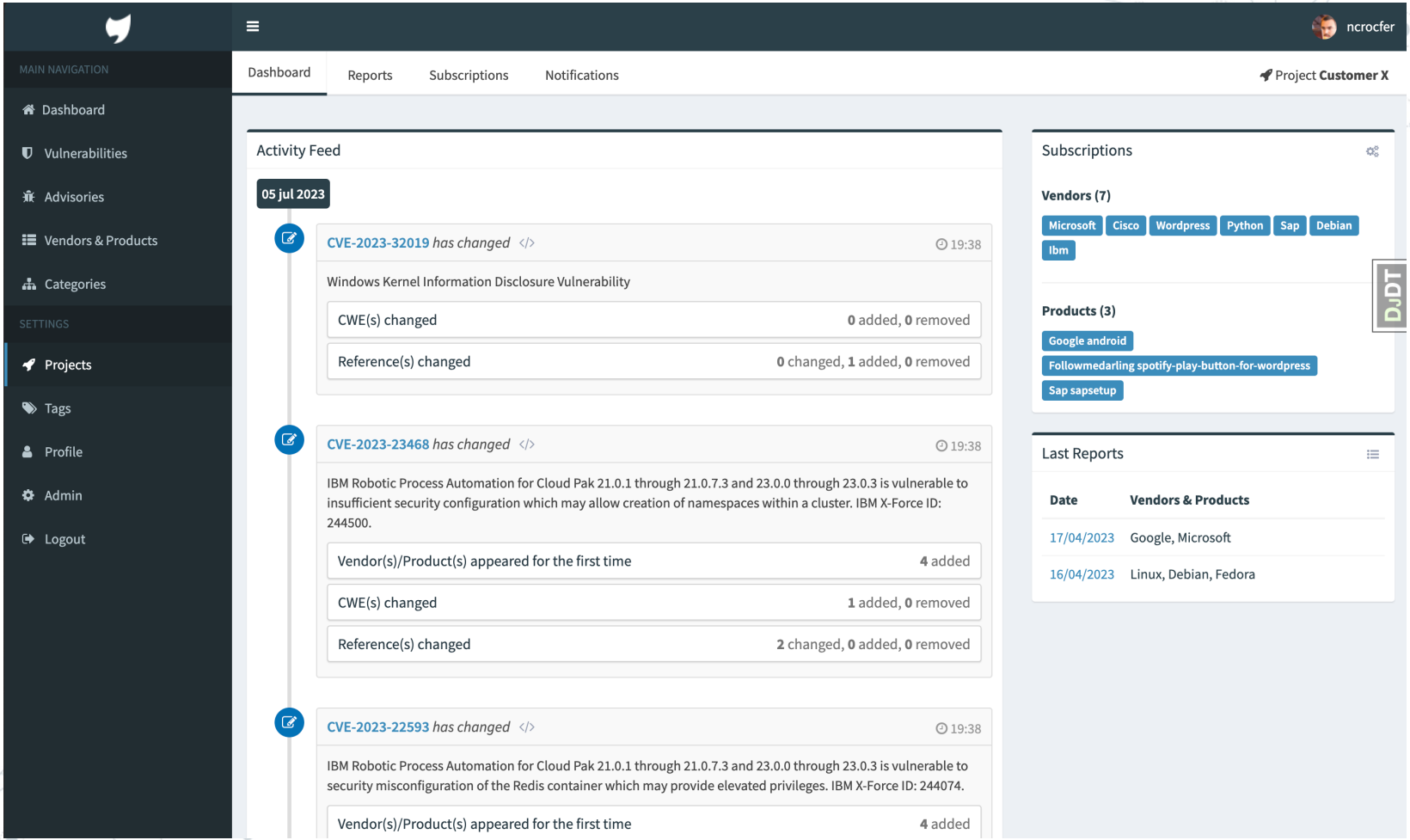
Présentation de la prochaine version

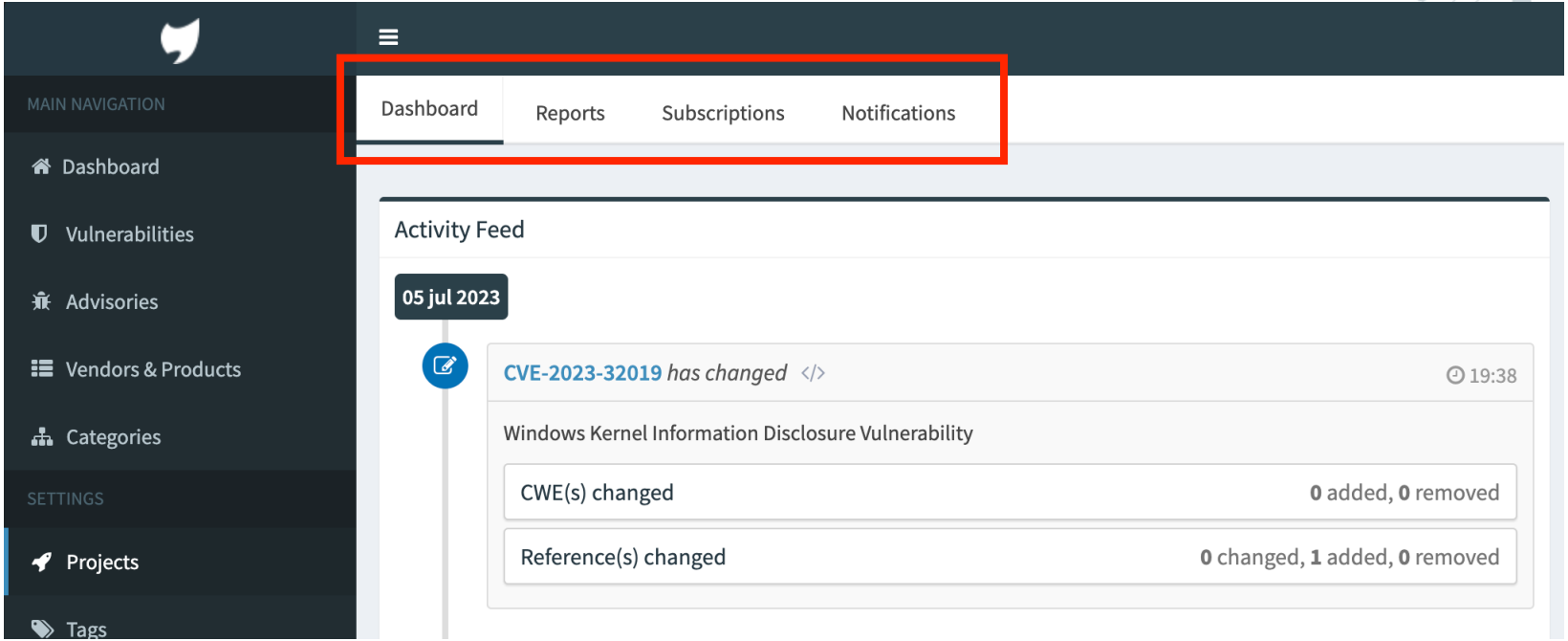
OpenCVE v2 – Nouvelles fonctionnalités

- Découpage des abonnements (vendors & products) en **Projets**
- **Notifications** (email, slack, jira, webhook…)
- Utilisation des bases du **NVD** et du **MITRE** *(cveproject/cvelistv5)*
- Ajout des **advisories** (Debian Security Advisories, Japan Vulnerability Notes, Ubuntu Security Notices, ExploitDB, Github Advisory Database…)
- La **knowledge-base** sur Github

OpenCVE v2 – Nouvelles fonctionnalités

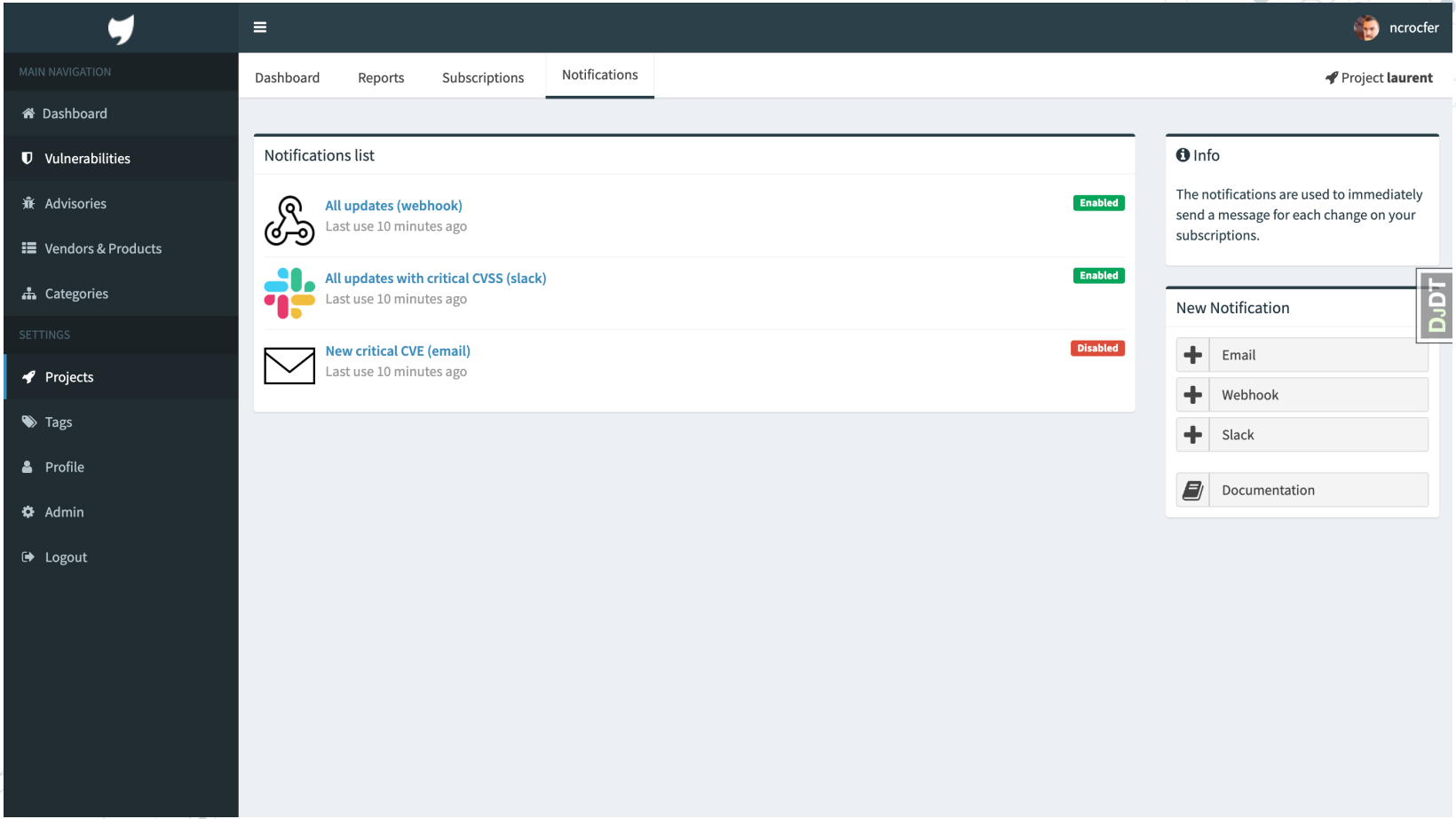
- Découpage des abonnements (vendors & products) en **Projets**
- **Notifications** (email, slack, jira, webhook…)
- Utilisation des bases du **NVD** et du **MITRE** *(cveproject/cvelistv5)*
- Ajout des **advisories** (Debian Security Advisories, Japan Vulnerability Notes, Ubuntu Security Notices, ExploitDB, Github Advisory Database…)
- La **knowledge-base** sur Github

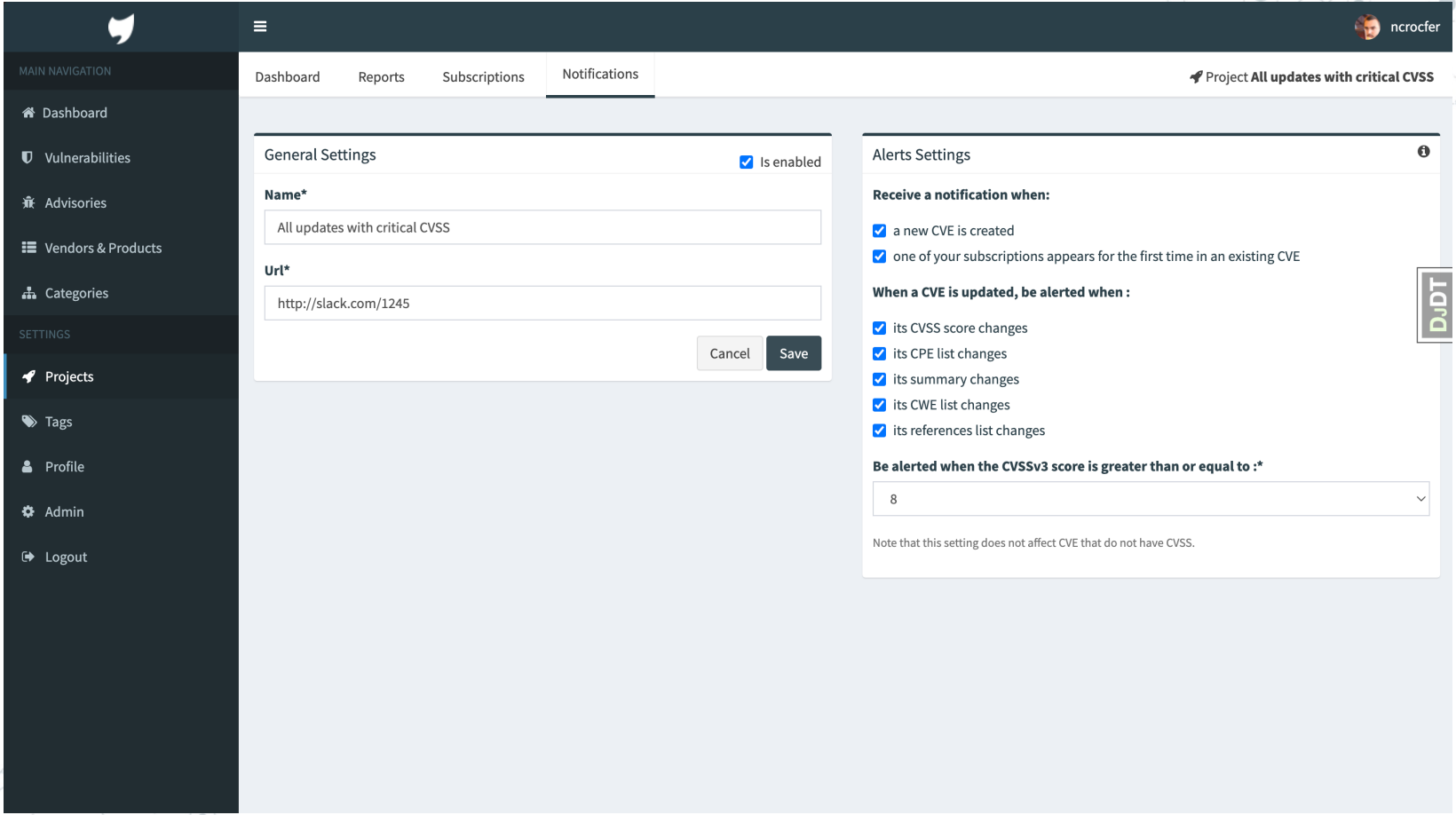

ncrocfer
MAIN NAVIGATION
Dashboard
Vulnerabilities
Advisories
Vendors & Products
Categories
SETTINGS
Projects
Tags
Profile
Admin
Logout
Dashboard
Reports
Subscriptions
Notifications
Project Customer X
Activity Feed
05 jul 2023
CVE-2023-32019 has changed
19:38
Windows Kernel Information Disclosure Vulnerability
CWE(s) changed
0 added, 0 removed
Reference(s) changed
0 changed, 1 added, 0 removed
CVE-2023-23468 has changed
19:38
IBM Robotic Process Automation for Cloud Pak 21.0.1 through 21.0.7.3 and 23.0.0 through 23.0.3 is vulnerable to insufficient security configuration which may allow creation of namespaces within a cluster. IBM X-Force ID: 244500.
Vendor(s)/Product(s) appeared for the first time
4 added
CWE(s) changed
1 added, 0 removed
Reference(s) changed
2 changed, 0 added, 0 removed
CVE-2023-22593 has changed
19:38
IBM Robotic Process Automation for Cloud Pak 21.0.1 through 21.0.7.3 and 23.0.0 through 23.0.3 is vulnerable to security misconfiguration of the Redis container which may provide elevated privileges. IBM X-Force ID: 244074.
Vendor(s)/Product(s) appeared for the first time
4 added
Subscriptions
Vendors (7)
Microsoft
Cisco
Wordpress
Python
Sap
Debian
Ibm
Products (3)
Google android
Followmedarling spotify-play-button-for-wordpress
Sap sapsetup
Last Reports
Date
Vendors & Products
17/04/2023
Google, Microsoft
16/04/2023
Linux, Debian, Fedora


MAIN NAVIGATION
Dashboard
Vulnerabilities
Advisories
Vendors & Products
Categories
SETTINGS
Projects
Tags
Dashboard
Reports
Subscriptions
Notifications
Activity Feed
05 jul 2023
CVE-2023-32019 has changed
19:38
Windows Kernel Information Disclosure Vulnerability
CWE(s) changed
0 added, 0 removed
Reference(s) changed
0 changed, 1 added, 0 removed

OpenCVE v2 – Nouvelles fonctionnalités

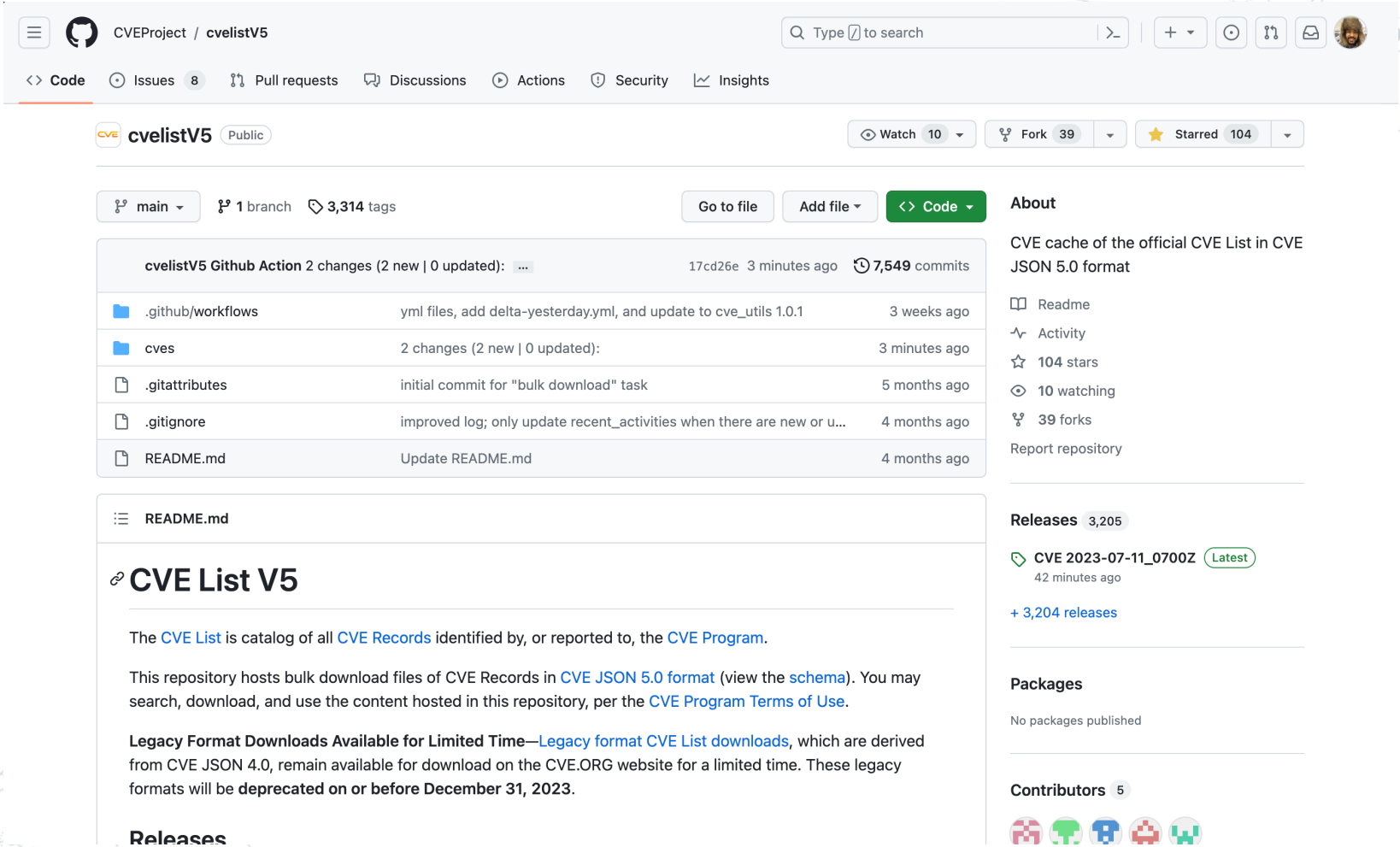
- Découpage des abonnements (vendors & products) en **Projets**
- **Notifications** (email, slack, jira, webhook…)
- Utilisation des bases du **NVD** et du **MITRE** *(cveproject/cvelistv5)*
- Ajout des **advisories** (Debian Security Advisories, Japan Vulnerability Notes, Ubuntu Security Notices, ExploitDB, Github Advisory Database…)
- La **knowledge-base** sur Github


ncrocfer
MAIN NAVIGATION
Dashboard
Vulnerabilities
Advisories
Vendors & Products
Categories
SETTINGS
Projects
Tags
Profile
Admin
Logout
Dashboard
Reports
Subscriptions
Notifications
Project laurent
Notifications list
All updates (webhook)
Last use 10 minutes ago
Enabled
All updates with critical CVSS (slack)
Last use 10 minutes ago
Enabled
New critical CVE (email)
Last use 10 minutes ago
Disabled
Info
The notifications are used to immediately send a message for each change on your subscriptions.
New Notification
Email
Webhook
Slack
Documentation


ncrocfer
MAIN NAVIGATION
Dashboard
Vulnerabilities
Advisories
Vendors & Products
Categories
SETTINGS
Projects
Tags
Profile
Admin
Logout
Dashboard
Reports
Subscriptions
Notifications
Project All updates with critical CVSS
General Settings
Is enabled
Name*
All updates with critical CVSS
Url*
http://slack.com/1245
Cancel
Save
Alerts Settings
Receive a notification when:
a new CVE is created
one of your subscriptions appears for the first time in an existing CVE
When a CVE is updated, be alerted when :
its CVSS score changes
its CPE list changes
its summary changes
its CWE list changes
its references list changes
Be alerted when the CVSSv3 score is greater than or equal to :*
8
Note that this setting does not affect CVE that do not have CVSS.
DJDT

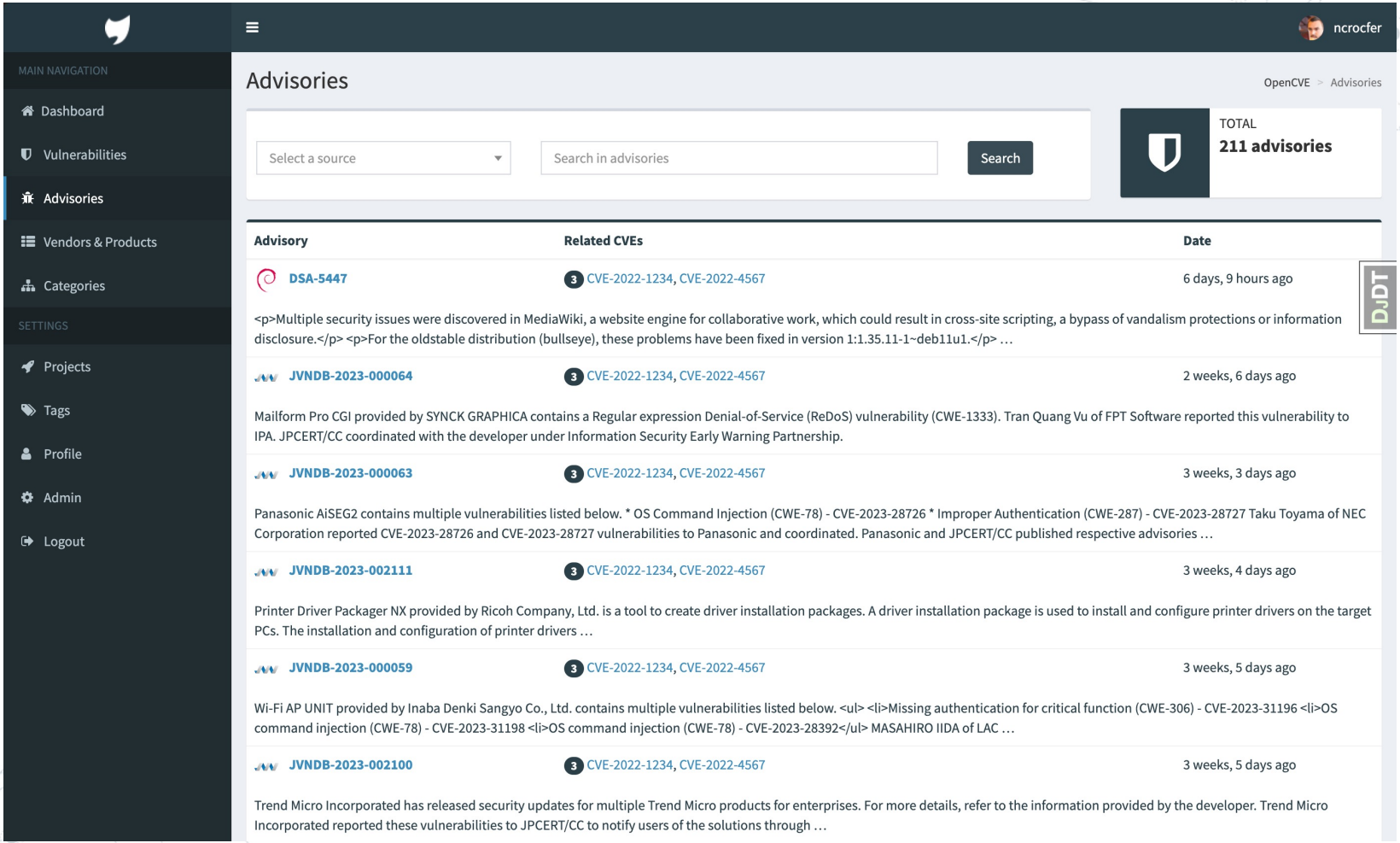
OpenCVE v2 – Nouvelles fonctionnalités

- Découpage des abonnements (vendors & products) en **Projets**
- **Notifications** (email, slack, jira, webhook…)
- Utilisation des bases du **NVD** et du **MITRE** *(cveproject/cvelistv5)*
- Ajout des **advisories** (Debian Security Advisories, Japan Vulnerability Notes, Ubuntu Security Notices, ExploitDB, Github Advisory Database…)
- La **knowledge-base** sur Github


CVEProject / cvelistV5
Type / to search
Code
Issues 8
Pull requests
Discussions
Actions
Security
Insights
cvelistV5 Public
Watch 10
Fork 39
Starred 104
main
1 branch
3,314 tags
Go to file
Add file
Code
cvelistV5 Github Action 2 changes (2 new | 0 updated): ...
17cd26e 3 minutes ago
7,549 commits
.github/workflows
yml files, add delta-yesterday.yml, and update to cve_utils 1.0.1
3 weeks ago
cves
2 changes (2 new | 0 updated):
3 minutes ago
.gitattributes
initial commit for "bulk download" task
5 months ago
.gitignore
improved log; only update recent_activities when there are new or u...
4 months ago
README.md
Update README.md
4 months ago
README.md
CVE List V5
The CVE List is catalog of all CVE Records identified by, or reported to, the CVE Program.
This repository hosts bulk download files of CVE Records in CVE JSON 5.0 format (view the schema). You may search, download, and use the content hosted in this repository, per the CVE Program Terms of Use.
Legacy Format Downloads Available for Limited Time—Legacy format CVE List downloads, which are derived from CVE JSON 4.0, remain available for download on the CVE.ORG website for a limited time. These legacy formats will be deprecated on or before December 31, 2023.
Releases
About
CVE cache of the official CVE List in CVE JSON 5.0 format
Readme
Activity
104 stars
10 watching
39 forks
Report repository
Releases 3,205
CVE 2023-07-11_0700Z Latest
42 minutes ago
+ 3,204 releases
Packages
No packages published
Contributors 5

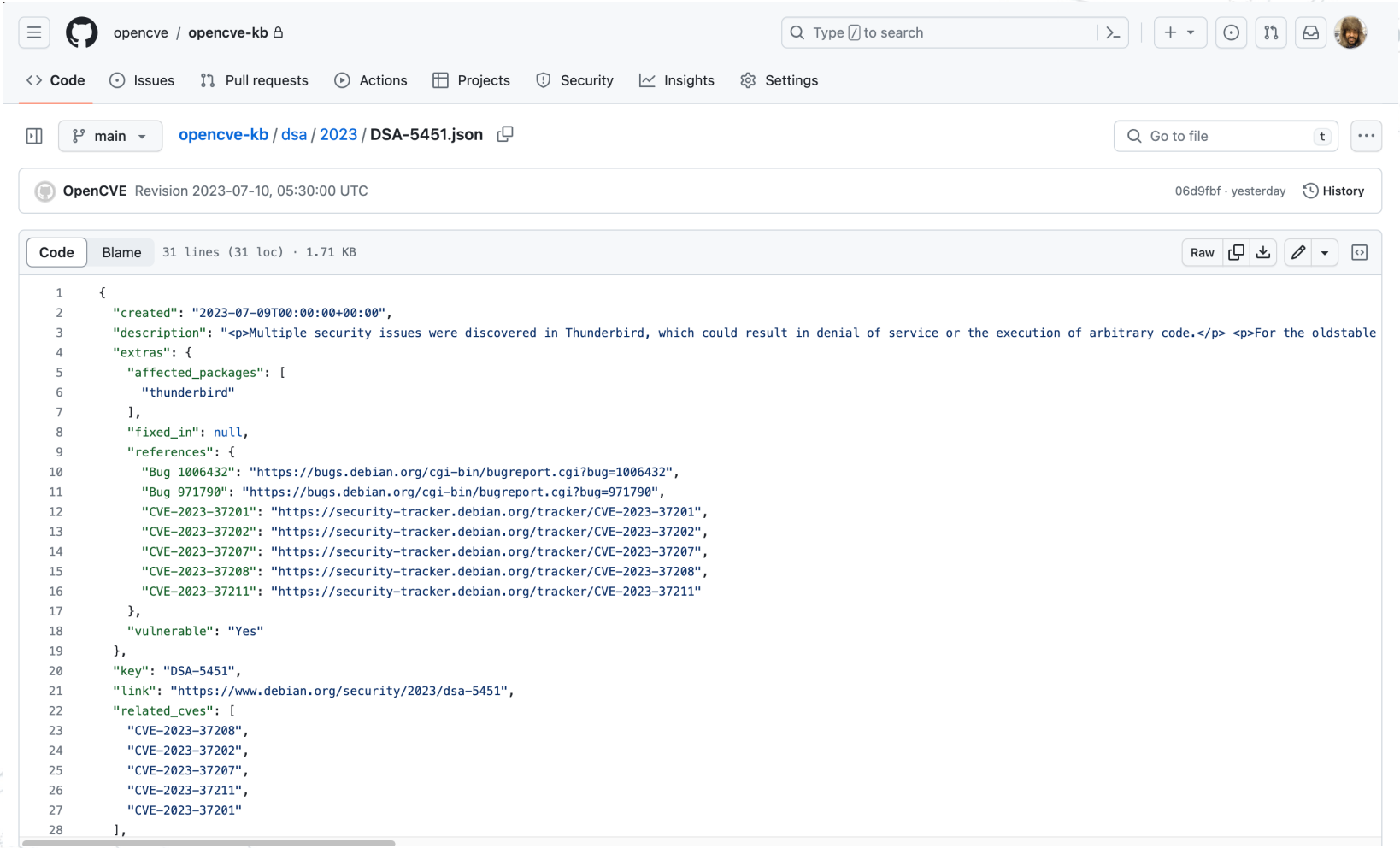
OpenCVE v2 – Nouvelles fonctionnalités

- Découpage des abonnements (vendors & products) en **Projets**
- **Notifications** (email, slack, jira, webhook…)
- Utilisation des bases du **NVD** et du **MITRE** *(cveproject/cvelistv5)*
- Ajout des **advisories** (Debian Security Advisories, Japan Vulnerability Notes, Ubuntu Security Notices, ExploitDB, Github Advisory Database…)
- La **knowledge-base** sur Github


ncrocfer
MAIN NAVIGATION
Dashboard
Vulnerabilities
Advisories
Vendors & Products
Categories
SETTINGS
Projects
Tags
Profile
Admin
Logout
Advisories
OpenCVE > Advisories
Select a source
Search in advisories
Search
TOTAL
211 advisories
Advisory
Related CVEs
Date
DSA-5447
3 CVE-2022-1234, CVE-2022-4567
6 days, 9 hours ago
Multiple security issues were discovered in MediaWiki, a website engine for collaborative work, which could result in cross-site scripting, a bypass of vandalism protections or information disclosure. For the oldstable distribution (bullseye), these problems have been fixed in version 1:1.35.11-1~deb11u1. …
JVNDB-2023-000064
3 CVE-2022-1234, CVE-2022-4567
2 weeks, 6 days ago
Mailform Pro CGI provided by SYNCK GRAPHICA contains a Regular expression Denial-of-Service (ReDoS) vulnerability (CWE-1333). Tran Quang Vu of FPT Software reported this vulnerability to IPA. JPCERT/CC coordinated with the developer under Information Security Early Warning Partnership.
JVNDB-2023-000063
3 CVE-2022-1234, CVE-2022-4567
3 weeks, 3 days ago
Panasonic AiSEG2 contains multiple vulnerabilities listed below. * OS Command Injection (CWE-78) - CVE-2023-28726 * Improper Authentication (CWE-287) - CVE-2023-28727 Taku Toyama of NEC Corporation reported CVE-2023-28726 and CVE-2023-28727 vulnerabilities to Panasonic and coordinated. Panasonic and JPCERT/CC published respective advisories …
JVNDB-2023-002111
3 CVE-2022-1234, CVE-2022-4567
3 weeks, 4 days ago
Printer Driver Packager NX provided by Ricoh Company, Ltd. is a tool to create driver installation packages. A driver installation package is used to install and configure printer drivers on the target PCs. The installation and configuration of printer drivers …
JVNDB-2023-000059
3 CVE-2022-1234, CVE-2022-4567
3 weeks, 5 days ago
Wi-Fi AP UNIT provided by Inaba Denki Sangyo Co., Ltd. contains multiple vulnerabilities listed below. Missing authentication for critical function (CWE-306) - CVE-2023-31196 OS command injection (CWE-78) - CVE-2023-31198 OS command injection (CWE-78) - CVE-2023-28392 MASAHIRO IIDA of LAC …
JVNDB-2023-002100
3 CVE-2022-1234, CVE-2022-4567
3 weeks, 5 days ago
Trend Micro Incorporated has released security updates for multiple Trend Micro products for enterprises. For more details, refer to the information provided by the developer. Trend Micro Incorporated reported these vulnerabilities to JPCERT/CC to notify users of the solutions through …
DJDT

OpenCVE v2 – Nouvelles fonctionnalités

- Découpage des abonnements (vendors & products) en **Projets**
- **Notifications** (email, slack, jira, webhook…)
- Utilisation des bases du **NVD** et du **MITRE** *(cveproject/cvelistv5)*
- Ajout des **advisories** (Debian Security Advisories, Japan Vulnerability Notes, Ubuntu Security Notices, ExploitDB, Github Advisory Database…)
- La **knowledge-base** sur Github

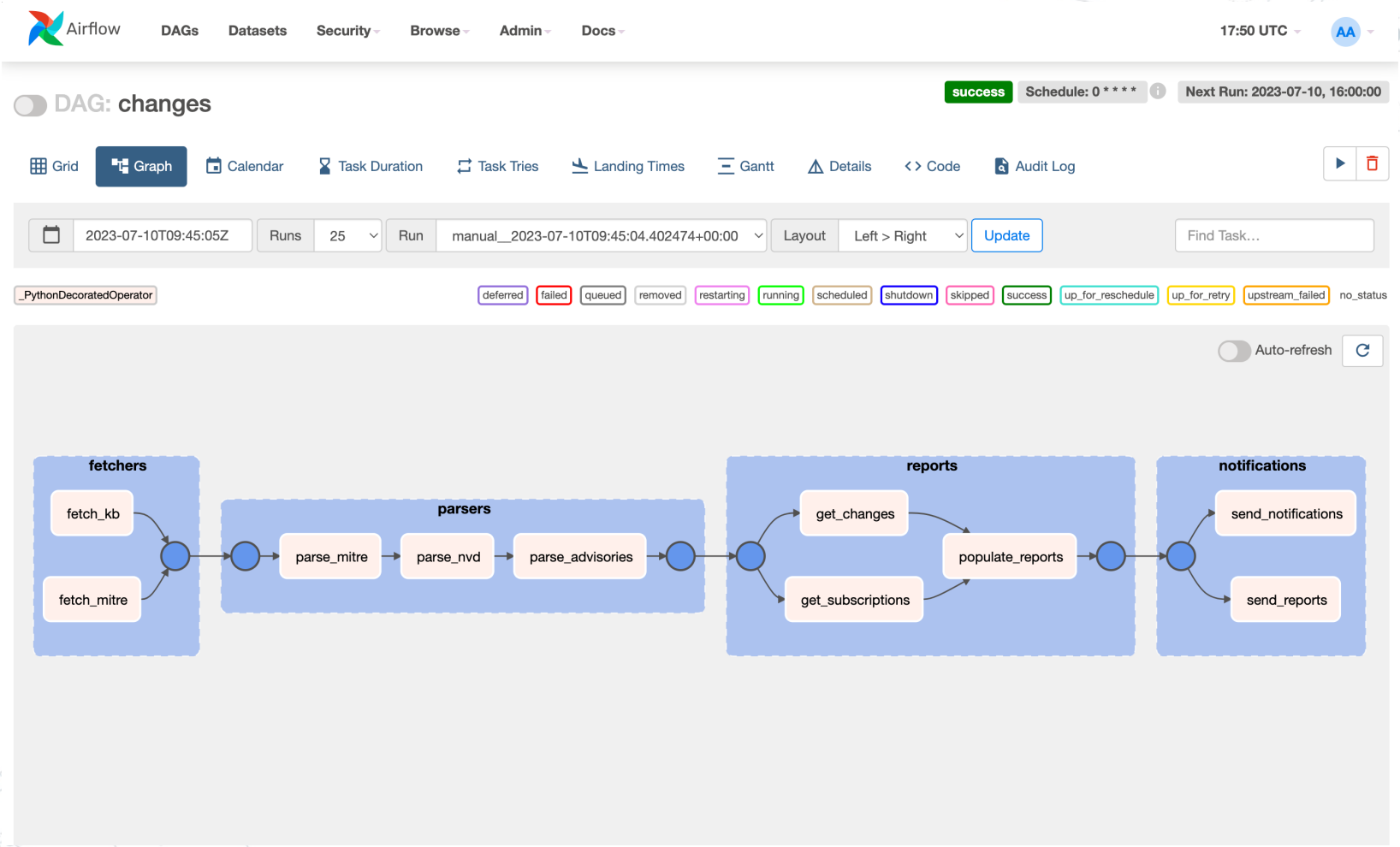

opencve / opencve-kb
Type / to search
Code
Issues
Pull requests
Actions
Projects
Security
Insights
Settings
main
opencve-kb / dsa / 2023 / DSA-5451.json
Go to file
t
OpenCVE Revision 2023-07-10, 05:30:00 UTC
06d9fbf · yesterday
History
Code
Blame
31 lines (31 loc) · 1.71 KB
Raw
{
"created": "2023-07-09T00:00:00+00:00",
"description": " Multiple security issues were discovered in Thunderbird, which could result in denial of service or the execution of arbitrary code. For the oldstable
"extras": {
"affected_packages": [
"thunderbird"
],
"fixed_in": null,
"references": {
"Bug 1006432": "https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1006432",
"Bug 971790": "https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=971790",
"CVE-2023-37201": "https://security-tracker.debian.org/tracker/CVE-2023-37201",
"CVE-2023-37202": "https://security-tracker.debian.org/tracker/CVE-2023-37202",
"CVE-2023-37207": "https://security-tracker.debian.org/tracker/CVE-2023-37207",
"CVE-2023-37208": "https://security-tracker.debian.org/tracker/CVE-2023-37208",
"CVE-2023-37211": "https://security-tracker.debian.org/tracker/CVE-2023-37211"
},
"vulnerable": "Yes"
},
"key": "DSA-5451",
"link": "https://www.debian.org/security/2023/dsa-5451",
"related_cves": [
"CVE-2023-37208",
"CVE-2023-37202",
"CVE-2023-37207",
"CVE-2023-37211",
"CVE-2023-37201"
],

OpenCVE v2 – Les technologies

- Réécriture complète de l'application web (de Flask à **Django**)
- Passage d'un micro-framework à un framework complet et maintenable
- Avantages: sécurité, extensions, documentation, communauté, auto-admin, ORM…

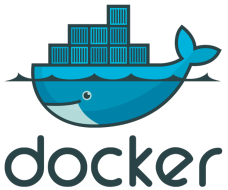
OpenCVE v2 – Les technologies

- Utilisation d'**Apache Airflow** comme scheduler
- Chaque heure Airflow lance les *workflows*:
  1. analyse des changements
  2. corrélation avec les abonnements des utilisateurs
  3. envoie de notifications et de rapports

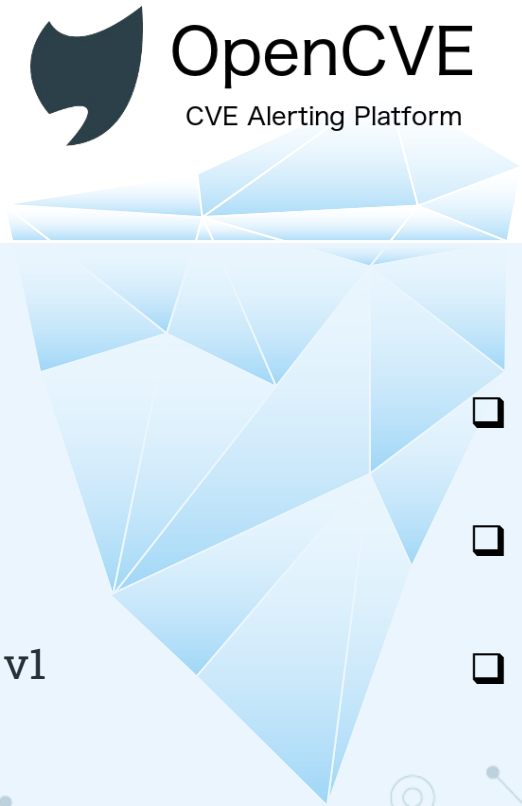

Airflow
DAGs
Datasets
Security
Browse
Admin
Docs
17:50 UTC
AA
DAG: changes
success
Schedule: 0 * * * *
Next Run: 2023-07-10, 16:00:00
Grid
Graph
Calendar
Task Duration
Task Tries
Landing Times
Gantt
Details
Code
Audit Log
2023-07-10T09:45:05Z
Runs
25
Run
manual__2023-07-10T09:45:04.402474+00:00
Layout
Left > Right
Update
Find Task...
_PythonDecoratedOperator
deferred
failed
queued
removed
restarting
running
scheduled
shutdown
skipped
success
up_for_reschedule
up_for_retry
upstream_failed
no_status
Auto-refresh
fetchers
fetch_kb
fetch_mitre
parsers
parse_mitre
parse_nvd
parse_advisories
reports
get_changes
get_subscriptions
populate_reports
notifications
send_notifications
send_reports

OpenCVE v2 – Les technologies

- Utilisation de **PostgreSQL** pour la base de données (procédures stockées)
- Utilisation de **Git** pour stocker la KB
- Utilisation de **Redis** dans le scheduler
- Utilisation de **Docker** pour le déploiement



Les prochaines étapes



- ❑ Création de la SAS
- ❑ Recherche de sponsors
- ❑ Finaliser la v2 / Migrer v1
- ❑ Communication / Articles
- ❑ Recueil de Feedbacks
- ❑ Bugfix / Nouvelles features

Merci !

https://www.opencve.io

ncrocfer@gmail.com

https://www.linkedin.com/in/nicolascrocfer/

https://twitter.com/ncrocfer