DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 29-03-2025

BULLETIN ALERTES

Object	Multiples vulnérabilités dans les produits Splunk
Réference	1337
Date de Publication	2025-03-28
Sévérité	Elevé

IMPACT :

- Exécution de code arbitraire à distance
- Accès à des données confidentielles
- Déni de service à distance

SYSTÉME AFFECTÉ :

- Splunk Cloud Platform versions 9.2.2406.10x antérieures à la version 9.2.2406.113
- Splunk Enterprise versions 9.3.x antérieures à la version 9.3.3
- Splunk Secure Gateway versions 3.8.x antérieures à la version 3.8.38
- Splunk Enterprise versions 9.4.x antérieures à la version 9.4.1
- Splunk Secure Gateway versions 3.7.x antérieures à la version 3.7.23
- Splunk Cloud Platform versions 9.1.x antérieures à la version 9.1.2312.208
- Splunk Infrastructure Monitoring Add-on versions antérieures à la version 1.2.7
- Splunk DB Connect versions antérieures à la version 4.0.0
- Splunk Enterprise versions 9.1.x antérieures à la version 9.1.8
- Splunk App for Lookup File Editing versions 4.0.x antérieures à la version 4.0.5
- Splunk Cloud Platform versions 9.3.2408.10x antérieures à la version 9.3.2408.107
- Splunk Enterprise versions 9.2.x antérieures à la version 9.2.5
- Splunk App for Data Science and Deep Learning versions 5.1.x antérieures à la version 5.2.0
- Splunk Add-on for Microsoft Cloud Services versions 5.4.x antérieures à la version 5.4.3
- Splunk Cloud Platform versions 9.2.x antérieures à la version 9.2.2403.115

DÉSCRIPTION :

Splunk a identifié plusieurs vulnérabilités majeures affectant ses produits. Leur exploitation pourrait permettre à un attaquant distant d’exécuter du code arbitraire, d’accéder à des données sensibles ou de provoquer un déni de service.

SOLUTION :

Mettre à jour les produits Splunk (se référer à la documentation).

DOCUMENTATION :

- Bulletins de sécurité de Splunk :

https://advisory.splunk.com/advisories/SVD-2025-0301

https://advisory.splunk.com/advisories/SVD-2025-0302

https://advisory.splunk.com/advisories/SVD-2025-0303

https://advisory.splunk.com/advisories/SVD-2025-0304

https://advisory.splunk.com/advisories/SVD-2025-0305

https://advisory.splunk.com/advisories/SVD-2025-0306

https://advisory.splunk.com/advisories/SVD-2025-0307

https://advisory.splunk.com/advisories/SVD-2025-0308

https://advisory.splunk.com/advisories/SVD-2025-0309

https://advisory.splunk.com/advisories/SVD-2025-0310

https://advisory.splunk.com/advisories/SVD-2025-0311

https://advisory.splunk.com/advisories/SVD-2025-0312

https://advisory.splunk.com/advisories/SVD-2025-0313

- CVE-2023-5363 :

https://nvd.nist.gov/vuln/detail/CVE-2023-5363

- CVE-2024-21090 :

https://nvd.nist.gov/vuln/detail/CVE-2024-21090

- CVE-2024-21272 :

https://nvd.nist.gov/vuln/detail/CVE-2024-21272

- CVE-2024-2511 :

https://nvd.nist.gov/vuln/detail/CVE-2024-2511

- CVE-2024-29857 :

https://nvd.nist.gov/vuln/detail/CVE-2024-29857

- CVE-2024-365 :

https://nvd.nist.gov/vuln/detail/CVE-2024-3651

- CVE-2024-38999 :

https://nvd.nist.gov/vuln/detail/CVE-2024-38999

- CVE-2024-39338 :

https://nvd.nist.gov/vuln/detail/CVE-2024-39338

- CVE-2024-45801 :

https://nvd.nist.gov/vuln/detail/CVE-2024-45801

- CVE-2024-4603 :

https://nvd.nist.gov/vuln/detail/CVE-2024-4603

- CVE-2024-47875 :

https://nvd.nist.gov/vuln/detail/CVE-2024-47875

- CVE-2024-6923 :

https://nvd.nist.gov/vuln/detail/CVE-2024-6923

- CVE-2025-20226 :

https://nvd.nist.gov/vuln/detail/CVE-2025-20226

- CVE-2025-20227

https://nvd.nist.gov/vuln/detail/CVE-2025-20227

- CVE-2025-20228 :

https://nvd.nist.gov/vuln/detail/CVE-2025-20228

- CVE-2025-20229 :

https://nvd.nist.gov/vuln/detail/CVE-2025-20229

- CVE-2025-20230 :

https://nvd.nist.gov/vuln/detail/CVE-2025-20230

- CVE-2025-20231 :

https://nvd.nist.gov/vuln/detail/CVE-2025-20231

- CVE-2025-20232 :

https://nvd.nist.gov/vuln/detail/CVE-2025-20232

- CVE-2025-20233 :

https://nvd.nist.gov/vuln/detail/CVE-2025-20233