ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques affectant plusieurs produits Splunk
Numéro de Référence	43560109/23
Date de Publication	01 Septembre 2023
Risque	Important
Impact	Critique

Systèmes affectés

- Splunk Cloud versions antérieures à 9.0.2305.200
- Splunk Enterprise versions 8.2.x antérieures à 8.2.12
- Splunk Enterprise versions 9.0.x antérieures à 9.0.6
- Splunk Enterprise versions 9.1.x antérieures à 9.1.1
- Splunk ITSI versions 4.13.x antérieures à 4.13.3
- Splunk ITSI versions 4.15.x antérieures à 4.15.3
- Universal Forwarder versions 8.2.x antérieures à 8.2.12
- Universal Forwarder versions 9.0.x antérieures à 9.0.6
- Universal Forwarder versions 9.1.x antérieures à 9.1.1

Identificateurs externes

CVE-2013-7489 CVE-2018-10237 CVE-2018-20225 CVE-2019-20454 CVE-2019-20838
CVE-2020-14155 CVE-2020-28469 CVE-2020-28851 CVE-2020-29652 CVE-2020-8169
CVE-2020-8177 CVE-2020-8231 CVE-2020-8284 CVE-2020-8285 CVE-2020-8286
CVE-2020-8908 CVE-2021-20066 CVE-2021-22569 CVE-2021-22876 CVE-2021-22890
CVE-2021-22897 CVE-2021-22898 CVE-2021-22901 CVE-2021-22922 CVE-2021-22923
CVE-2021-22924 CVE-2021-22925 CVE-2021-22926 CVE-2021-22945 CVE-2021-22946
CVE-2021-22947 CVE-2021-23343 CVE-2021-23382 CVE-2021-27918 CVE-2021-27919
CVE-2021-29060 CVE-2021-29425 CVE-2021-29923 CVE-2021-30560 CVE-2021-31525
CVE-2021-31566 CVE-2021-33194 CVE-2021-33195 CVE-2021-33196 CVE-2021-33197
CVE-2021-33198 CVE-2021-34558 CVE-2021-3520 CVE-2021-3572 CVE-2021-36221
CVE-2021-36976 CVE-2021-3803 CVE-2021-38297 CVE-2021-38561 CVE-2021-39293

CVE-2021-41182 CVE-2021-41183 CVE-2021-41184 CVE-2021-41771 CVE-2021-41772
CVE-2021-43565 CVE-2021-44716 CVE-2021-44717 CVE-2022-1705 CVE-2022-1941
CVE-2022-1962 CVE-2022-22576 CVE-2022-2309 CVE-2022-23491 CVE-2022-23772
CVE-2022-23773 CVE-2022-23806 CVE-2022-24675 CVE-2022-24921 CVE-2022-24999
CVE-2022-25881 CVE-2022-27191 CVE-2022-27536 CVE-2022-27664 CVE-2022-27774
CVE-2022-27775 CVE-2022-27776 CVE-2022-27778 CVE-2022-27779 CVE-2022-27780
CVE-2022-27781 CVE-2022-27782 CVE-2022-28131 CVE-2022-28327 CVE-2022-2879
CVE-2022-2880 CVE-2022-29526 CVE-2022-29804 CVE-2022-30115 CVE-2022-30580
CVE-2022-30629 CVE-2022-30630 CVE-2022-30631 CVE-2022-30632 CVE-2022-30633
CVE-2022-30634 CVE-2022-30635 CVE-2022-31129 CVE-2022-3171 CVE-2022-32148
CVE-2022-32149 CVE-2022-32189 CVE-2022-32205 CVE-2022-32206 CVE-2022-32207
CVE-2022-32208 CVE-2022-32221 CVE-2022-33987 CVE-2022-3509 CVE-2022-3510
CVE-2022-3517 CVE-2022-35252 CVE-2022-35260 CVE-2022-35737 CVE-2022-36227
CVE-2022-37599 CVE-2022-37601 CVE-2022-37603 CVE-2022-38900 CVE-2022-40023
CVE-2022-40897 CVE-2022-40899 CVE-2022-41715 CVE-2022-41716 CVE-2022-41720
CVE-2022-41722 CVE-2022-42003 CVE-2022-42004 CVE-2022-42915 CVE-2022-42916
CVE-2022-43551 CVE-2022-43552 CVE-2022-46175 CVE-2023-23914 CVE-2023-23915
CVE-2023-23916 CVE-2023-24539 CVE-2023-24540 CVE-2023-27533 CVE-2023-27534
CVE-2023-27535 CVE-2023-27536 CVE-2023-27537 CVE-2023-27538 CVE-2023-29400
CVE-2023-29402 CVE-2023-29403 CVE-2023-29404 CVE-2023-29405 CVE-2023-2976
CVE-2023-40592 CVE-2023-40593 CVE-2023-40594 CVE-2023-40595 CVE-2023-40596
CVE-2023-40597 CVE-2023-40598 CVE-2023-4571

Bilan de la vulnérabilité

Splunk annonce la correction de plusieurs vulnérabilités critiques affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire, de contourner les mesures de sécurité ou de causer un déni de service.

Solution

Veuillez se référer aux bulletins de sécurité de l'éditeur pour l'obtention du correctif.

Risque

- Exécution de code arbitraire à distance
- Contournement de mesures de sécurité
- Déni de service à distance

Références

Bulletins de sécurité de Splunk :

- https://advisory.splunk.com/advisories/SVD-2023-0801
- https://advisory.splunk.com/advisories/SVD-2023-0801
- https://advisory.splunk.com/advisories/SVD-2023-0802
- https://advisory.splunk.com/advisories/SVD-2023-0803
- https://advisory.splunk.com/advisories/SVD-2023-0804
- https://advisory.splunk.com/advisories/SVD-2023-0805
- https://advisory.splunk.com/advisories/SVD-2023-0806
- https://advisory.splunk.com/advisories/SVD-2023-0807
- https://advisory.splunk.com/advisories/SVD-2023-0808
- https://advisory.splunk.com/advisories/SVD-2023-0809
- https://advisory.splunk.com/advisories/SVD-2023-0810
- https://advisory.splunk.com/advisories/SVD-2023-0811

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma