ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits Siemens
Numéro de Référence	46521303/24
Date de Publication	13 Mars 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- Solid Edge versions antérieures à V223.0.11
- Siveillance Control versions supérieures ou égales à V2.8 versions antérieures à V3.1.1
- Sinteso Mobile versions antérieures à V3.0.0
- Sinteso FS20 EN X300 Cloud Distribution versions V4.3.x antérieures à V4.3.5617
- Sinteso FS20 EN X300 Cloud Distribution versions V4.2.x antérieures à V4.2.5015
- Sinteso FS20 EN X200 Cloud Distribution versions V4.3.x antérieures à V4.3.5618
- Sinteso FS20 EN X200 Cloud Distribution versions V4.0.x antérieures à V4.0.5016
- Sinteso FS20 EN Fire Panel FC20 versions antérieures à MP8
- Sinteso FS20 EN Engineering Tool versions antérieures à MP8
- SINEMA Remote Connect Server versions antérieures à V3.2
- SINEMA Remote Connect Client versions antérieures à V3.1 SP1
- SIMATIC RF160B (6GT2003-0FA00) versions antérieures à V2.2
- SENTRON 7KM PAC3220 DC (7KM3220-1BA01-1EA0) versions supérieures ou égales à V3.2.3 versions antérieures à V3.3.0
- SENTRON 7KM PAC3220 AC/DC (7KM3220-0BA01-1DA0) versions supérieures ou égales à V3.2.3 versions antérieures à V3.3.0
- SENTRON 7KM PAC3120 DC (7KM3120-1BA01-1EA0) versions supérieures ou égales à V3.2.3 versions antérieures à V3.3.0
- SENTRON 7KM PAC3120 AC/DC (7KM3120-0BA01-1DA0) versions supérieures ou égales à V3.2.3 versions antérieures à V3.3.0
- SENTRON 3KC ATC6 Expansion Module Ethernet toutes versions

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- RUGGEDCOM APE1808 avec Fortinet NGFW versions antérieures à V7.4.1
- Cerberus PRO EN X300 Cloud Distribution versions V4.3.x antérieures à V4.3.5617
- Cerberus PRO EN X300 Cloud Distribution versions V4.2.x antérieures à V4.2.5015
- Cerberus PRO EN X200 Cloud Distribution versions V4.3.x antérieures à V4.3.5618
- Cerberus PRO EN X200 Cloud Distribution versions V4.0.x antérieures à V4.0.5016
- Cerberus PRO EN Fire Panel FC72x versions antérieures à IP8
- Cerberus PRO EN Engineering Tool versions antérieures à IP8

Identificateurs externes

- CVE-2017-14491 CVE-2017-18509 CVE-2020-0338 CVE-2020-0417 CVE-2020-10768 CVE-2020-11301 CVE-2020-14305 CVE-2020-14381 CVE-2020-15436 CVE-2020-23064 CVE-2020-24587 CVE-2020-25705 CVE-2020-26555 CVE-2020-26558 CVE-2020-29660 CVE-2020-29661 CVE-2021-0302 CVE-2021-0305 CVE-2021-0325 CVE-2021-0326 CVE-2021-0327 CVE-2021-0328 CVE-2021-0329 CVE-2021-0330 CVE-2021-0331 CVE-2021-0333 CVE-2021-0334 CVE-2021-0336 CVE-2021-0337 CVE-2021-0339 CVE-2021-0341 CVE-2021-0390 CVE-2021-0391 CVE-2021-0392 CVE-2021-0393 CVE-2021-0394 CVE-2021-0396 CVE-2021-0397 CVE-2021-0399 CVE-2021-0400 CVE-2021-0429 CVE-2021-0431 CVE-2021-0433 CVE-2021-0434 CVE-2021-0435 CVE-2021-0436 CVE-2021-0437 CVE-2021-0438 CVE-2021-0443 CVE-2021-0444 CVE-2021-0471 CVE-2021-0473 CVE-2021-0474 CVE-2021-0476 CVE-2021-0478 CVE-2021-0480 CVE-2021-0481 CVE-2021-0484 CVE-2021-0506 CVE-2021-0507 CVE-2021-0508 CVE-2021-0509 CVE-2021-0510 CVE-2021-0511 CVE-2021-0512 CVE-2021-0513 CVE-2021-0514 CVE-2021-0515 CVE-2021-0516 CVE-2021-0519 CVE-2021-0520 CVE-2021-0521 CVE-2021-0522 CVE-2021-0584 CVE-2021-0585 CVE-2021-0586 CVE-2021-0587 CVE-2021-0588 CVE-2021-0589 CVE-2021-0591 CVE-2021-0593 CVE-2021-0594 CVE-2021-0596 CVE-2021-0597 CVE-2021-0598 CVE-2021-0599 CVE-2021-0600 CVE-2021-0601 CVE-2021-0604 CVE-2021-0640 CVE-2021-0641 CVE-2021-0642 CVE-2021-0646 CVE-2021-0650 CVE-2021-0651 CVE-2021-0652 CVE-2021-0653 CVE-2021-0682 CVE-2021-0683 CVE-2021-0684 CVE-2021-0687 CVE-2021-0688 CVE-2021-0689 CVE-2021-0690 CVE-2021-0692 CVE-2021-0695 CVE-2021-0704 CVE-2021-0706 CVE-2021-0708 CVE-2021-0870 CVE-2021-0919 CVE-2021-0920 CVE-2021-0926 CVE-2021-0928 CVE-2021-0929 CVE-2021-0930 CVE-2021-0931 CVE-2021-0933 CVE-2021-0952 CVE-2021-0953 CVE-2021-0961 CVE-2021-0963 CVE-2021-0964 CVE-2021-0965 CVE-2021-0967 CVE-2021-0968 CVE-2021-0970 CVE-2021-1972 CVE-2021-1976 CVE-2021-29647 CVE-2021-33909 CVE-2021-38204 CVE-2021-39621 CVE-2021-39623 CVE-2021-39626 CVE-2021-39627 CVE-2021-39629 CVE-2021-39633 CVE-2021-39634 CVE-2022-20127 CVE-2022-20130 CVE-2022-20227 CVE-2022-20229 CVE-2022-20355 CVE-2022-20411 CVE-2022-20421 CVE-2022-20422 CVE-2022-20423 CVE-2022-20462 CVE-2022-20466 CVE-2022-20468 CVE-2022-20469 CVE-2022-20472 CVE-2022-20473 CVE-2022-20476 CVE-2022-20483 CVE-2022-20498 CVE-2022-20500 CVE-2022-32257 CVE-2022-39948 CVE-2022-41327 CVE-2022-41328 CVE-2022-41329 CVE-2022-41330 CVE-2022-41334 CVE-2022-42469 CVE-2022-42474 CVE-2022-42476 CVE-2022-43947 CVE-2022-43953 CVE-2022-45861 CVE-2023-22639 CVE-2023-22640 CVE-2023-22641 CVE-2023-25610 CVE-2023-

26207 CVE-2023-27997 CVE-2023-28001 CVE-2023-28002 CVE-2023-29175 CVE-2023-29178 CVE-2023-29179 CVE-2023-29180 CVE-2023-29181 CVE-2023-29183 CVE-2023-33301 CVE-2023-33305 CVE-2023-33306 CVE-2023-33307 CVE-2023-33308 CVE-2023-36555 CVE-2023-36639 CVE-2023-36641 CVE-2023-37935 CVE-2023-38545 CVE-2023-38546 CVE-2023-40718 CVE-2023-41675 CVE-2023-41841 CVE-2023-44250 CVE-2023-44487 CVE-2023-45793 CVE-2023-47537 CVE-2023-49125 CVE-2024-21483 CVE-2024-21762 CVE-2024-22039 CVE-2024-22040 CVE-2024-22041 CVE-2024-22044 CVE-2024-22045 CVE-2024-23113

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les systèmes industriels de Siemens susmentionnés. Un attaquant pourrait exploiter ces failles afin d'exécuter du code arbitraire à distance, réussir une élévation de privilèges, causer un déni de service, contourner la politique de sécurité ou porter atteinte à la confidentialité de données.

Solution

Veuillez se référer au bulletin de sécurité Siemens du 12 Mars 2024 pour plus d'information.

Risque

- Exécution de code arbitraire à distance
- Elévation de privilèges
- Déni de service
- Contournement de la politique de sécurité
- Atteinte à la confidentialité de données

Annexe

Bulletin de sécurité Siemens du 12 Mars 2024:

- https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications