

CVE-2019-12959

Share

| |
|-----------------|
| CVE-2015-4596 |
| CVE-2015-5384 |
| CVE-2015-5462 |
| CVE-2015-5463 |
| CVE-2015-5606 |
| CVE-2016-1159 |
| CVE-2016-1161 |
| CVE-2017-1282 |
| CVE-2017-1331 |
| CVE-2018-10206 |
| CVE-2018-10207 |
| CVE-2018-10208 |
| CVE-2018-10209 |
| CVE-2018-10210 |
| CVE-2018-10211 |
| CVE-2018-10212 |
| CVE-2018-10213 |
| CVE-2018-15631 |
| CVE-2018-18466 |
| CVE-2018-20237 |
| CVE-2018-20664 |
| CVE-2018-20736 |
| CVE-2018-20737 |
| CVE-2019-11032 |
| CVE-2019-12959 |
| CVE-2019-12994 |
| CVE-2019-14693 |
| CVE-2019-16202 |
| CVE-2019-17112 |
| CVE-2019-19610 |
| CVE-2019-19611 |
| CVE-2019-19612 |
| CVE-2019-19613 |
| CVE-2019-19614 |
| CVE-2019-20474 |
| CVE-2019-3905 |
| CVE-2019-6512 |
| CVE-2019-6513 |
| CVE-2019-6514 |
| CVE-2019-6515 |
| CVE-2019-6516 |
| CVE-2019-6970 |
| CVE-2019-7161 |
| CVE-2019-7162 |
| CVE-2019-9676 |
| CVE-2020-15594 |
| CVE-2020-15595 |
| CVE-2020-26167 |
| CVE-2020-26546 |
| CVE-2020-28401 |
| CVE-2020-28402 |
| CVE-2020-28403 |
| CVE-2020-28404 |
| CVE-2020-28405 |
| CVE-2020-28406 |
| CVE-2020-28918 |
| CVE-2020-8422 |
| CVE-2021- 42110 |
| CVE-2021- 44035 |
| CVE-2021-31160 |
| CVE-2021-31399 |
| CVE-2021-31530 |
| CVE-2021-31531 |
| CVE-2021-31777 |
| CVE-2021-32016 |
| CVE-2021-32017 |
| CVE-2021-32018 |
| CVE-2021-38615 |
| CVE-2021-38616 |
| CVE-2021-38617 |
| CVE-2021-38618 |
| CVE-2021-41320 |
| CVE-2021-42111 |
| CVE-2021-43978 |
| CVE-2022-0028 |
| CVE-2022-21828 |
| CVE-2022-22571 |
| CVE-2022-22572 |
| CVE-2022-24446 |
| CVE-2022-24447 |
| CVE-2022-24967 |
| CVE-2022-29931 |
| CVE-2022-30332 |
| CVE-2022-34908 |
| CVE-2022-34909 |
| CVE-2022-34910 |
| CVE-2022-36441 |
| CVE-2022-36442 |
| CVE-2022-36443 |
| CVE-2022-37028 |
| CVE-2022-38481 |
| CVE-2022-38482 |
| CVE-2022-45164 |
| CVE-2022-45165 |
| CVE-2022-45166 |
| CVE-2022-45167 |
| CVE-2023-26097 |
| CVE-2023-26098 |
| CVE-2023-26099 |
| CVE-2023-27565 |
| CVE-2023-28150 |
| CVE-2023-28151 |
| CVE-2023-28152 |
| CVE-2023-29505 |
| CVE-2023-31223 |
| CVE-2023-35791 |
| CVE-2023-35792 |
| CVE-2023-41103 |
| CVE-2023-48644 |
| CVE-2023-48645 |
| CVE-2023-50872 |
| CVE-2023-51710 |
| CVE-2023-51711 |
| CVE-2024-24720 |
| CVE-2024-24721 |
| CVE-2024-25676 |
| CVE-2024-28060 |
| CVE-2024-28061 |
| CVE-2024-38815 |
| XLM-2016-121 |
| XLM-2018-356 |
| XLM-2019-672 |
| XLM-2019-712 |
| XLM-2020-1347 |
| XLM-2024-6203 |
| XLM-2024-6482 |
| XLM-2024-6483 |
| XLM-2024-6484 |

Abstract Advisory Information

A service exposed by the software allows to a basic user to perform a Server Side Request Forgery attack. This attack can also leveraged via a CSRF attack.

Authors: Dominique Righetto

Version affected

Name : AssetExplorer
Product version: 6.2.0

Common Vulnerability Scoring System

5.0
CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/CL:A/N/A:N

Patches

The vulnerability is patched in version 6.5 Build 6502

References

<https://www.manageengine.com/products/asset-explorer/sp-readme.html>

Vulnerability Disclosure Timeline

- 04-05-2019: Vulnerability identification
- 06-05-2019: First contact with the vendor
- 06-05-2019: Acknowledge from the vendor
- 24-06-2019: Vulnerability patched by vendor
- 25-06-2019: CVE assigned by Mitre
- 17-07-2019: Patch release by vendor
- 06-08-2019: Public disclosure

Let's deliver the right solution for your business

CONTACT US

Meet Success

About Us
Career Opportunities
Where to meet us
Privacy Notice
Contact Us

Services

Eyeguard
Information Security Governance
Intrusion Tests - Red Team
Application Security
Network & Security Infrastructure
CERT-XLM
Eyetools
Training

Follow us

