CERT-EU

## Security Advisory 2023-004

# Critical Vulnerability in Several ManageEngine Products

*January 30, 2023 — v1.0*

**TLP:CLEAR**

*History:*

- *30/01/2023 — v1.0 – Initial publication*

## Summary

On January 18th, ManageEngine released updates to several ManageEngine OnPremise products [1]. The potentially vulnerable products use outdated versions of the open-source library Apache Santuario (XML Security for Java). Products must have enabled Single-Sign-On (SSO) using the Security Assertion Markup Language (SAML) to be vulnerable. For some products, the SSO must be active, while for others, it is sufficient that SSO was active once. As a result, the vulnerability allows an unauthenticated adversary to execute arbitrary code. Additionally, a Proof-of-Concept exploit is available [2].

## Technical Details

ManageEngine uses different versions of Apache Santuario in various products. The vulnerability CVE-2022-47966 exploits the combination of two issues in the library's version below version 2.2.3.

The primary issue affects the SAML validation order. The vulnerable library performs reference validation before signature validation. This behaviour allows the injection of arbitrary XSL Transformations, which enables the attacker to execute arbitrary Java code [3,4].

Suppose Single-Sign-On (SSO) is enabled using the Security Assertion Markup Language (SAML). In that case, an attacker can exploit the vulnerability by sending a malicious SAML Response to the Assertion Consumer URL of the ManageEngine product. Based on the product, e.g., the AD-related products like AdManager, there might be additional checks on the SAML response. However, an attacker can bypass these checks without much extra effort.

## Affected Products

| Product Name | Impacted Version(s) | Fixed Version(s) | Released On |
|---|---|---|---|
| Access Manager Plus* | 4307 and below | 4308 | 7/11/2022 |
| Active Directory 360** | 4309 and below | 4310 | 28/10/2022 |
| ADAudit Plus** | 7080 and below | 7081 | 28/10/2022 |
| ADManager Plus** | 7161 and below | 7162 | 28/10/2022 |
| ADSelfService Plus** | 6210 and below | 6211 | 28/10/2022 |
| Analytics Plus* | 5140 and below | 5150 | 7/11/2022 |
| Application Control Plus* | 10.1.2220.17 and below | 10.1.2220.18 | 28/10/2022 |
| Asset Explorer** | 6982 and below | 6983 | 27/10/2022 |
| Browser Security Plus* | 11.1.2238.5 and below | 11.1.2238.6 | 28/10/2022 |
| Device Control Plus* | 10.1.2220.17 and below | 10.1.2220.18 | 28/10/2022 |
| Endpoint Central* | 10.1.2228.10 and below | 10.1.2228.11 | 28/10/2022 |
| Endpoint Central MSP* | 10.1.2228.10 and below | 10.1.2228.11 | 28/10/2022 |
| Endpoint DLP* | 10.1.2137.5 and below | 10.1.2137.6 | 28/10/2022 |
| Key Manager Plus* | 6400 and below | 6401 | 27/10/2022 |
| OS Deployer* | 1.1.2243.0 and below | 1.1.2243.1 | 28/10/2022 |
| PAM 360* | 5712 and below | 5713 | 7/11/2022 |
| Password Manager Pro* | 12123 and below | 12124 | 7/11/2022 |
| Patch Manager Plus* | 10.1.2220.17 and below | 10.1.2220.18 | 28/10/2022 |
| Remote Access Plus* | 10.1.2228.10 and below | 10.1.2228.11 | 28/10/2022 |
| Remote Monitoring and Management (RMM)* | 10.1.40 and below | 10.1.41 | 29/10/2022 |
| ServiceDesk Plus** | 14003 and below | 14004 | 27/10/2022 |
| ServiceDesk Plus MSP** | 13000 and below | 13001 | 27/10/2022 |
| SupportCenter Plus** | 11017 to 11025 | 11026 | 28/10/2022 |
| Vulnerability Manager Plus* | 10.1.2220.17 and below | 10.1.2220.18 | 28/10/2022 |

** - Applicable only if configured SAML-based SSO and it is currently active.*

*** - Applicable only if configured SAML-based SSO at least once in the past, regardless of the current SAML-based SSO status.*

## Recommendations

CERT-EU recommends to update potentially vulnerable products to the latest version.

Deactivating the SAML-based SSO configuration can be a short-term solution for applicable products until the update could be performed.

## References

[1] https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

[2] https://github.com/horizon3ai/CVE-2022-47966

[3] https://www.horizon3.ai/manageengine-cve-2022-47966-technical-deep-dive/

[4] https://blog.viettelcybersecurity.com/saml-show-stopper/