An official website of the United States government Here's how you know

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Archived Content

In an effort to keep CISA.gov current, the archive contains outdated information that may not reflect current policy or programs.

CYBERSECURITY ADVISORY

Critical Vulnerability in SAP NetWeaver AS Java

Last Revised: July 13, 2020 **Alert Code:** AA20-195A

Give Feedback

Summary

On July 13, 2020 EST, SAP released a security update to address a critical vulnerability, CVE-2020-6287, affecting the SAP NetWeaver Application Server (AS) Java component LM Configuration Wizard. An unauthenticated attacker can exploit this vulnerability through the Hypertext Transfer Protocol (HTTP) to take control of trusted SAP applications.

Due to the criticality of this vulnerability, the attack surface this vulnerability represents, and the importance of SAP's business applications, the Cybersecurity and Infrastructure Security Agency (CISA) strongly recommends organizations immediately apply patches. CISA recommends organizations prioritize patching internet-facing systems, and then internal systems.

Organizations that are unable to immediately patch should mitigate the vulnerability by disabling the LM Configuration Wizard service (see SAP Security Note #2939665 <https://launchpad.support.sap.com/#/notes/2939665>). Should these options be unavailable or if the actions will take more than 24 hours to complete, CISA strongly recommends closely monitoring your SAP NetWeaver AS for anomalous activity.

CISA is unaware of any active exploitation of these vulnerabilities at the time of this report. However, because patches have been publicly released, the underlying vulnerabilities could be reverse-engineered to create exploits that target unpatched systems.

Technical Details

Affected Systems

This vulnerability is present by default in SAP applications running on top of SAP NetWeaver AS Java 7.3 and any newer versions (up to SAP NetWeaver 7.5). Potentially vulnerable SAP business solutions include any SAP Java-based solutions such as (but not limited to):

- SAP Enterprise Resource Planning,
- SAP Product Lifecycle Management,
- SAP Customer Relationship Management,
- SAP Supply Chain Management,
- SAP Supplier Relationship Management,
- SAP NetWeaver Business Warehouse,
- SAP Business Intelligence,
- SAP NetWeaver Mobile Infrastructure,
- SAP Enterprise Portal,
- SAP Process Orchestration/Process Integration),
- SAP Solution Manager,
- SAP NetWeaver Development Infrastructure,

Give Feedback

- SAP Central Process Scheduling,
- SAP NetWeaver Composition Environment, and
- SAP Landscape Manager.

Attack Surface

The vulnerability was identified in a component that is part of the SAP NetWeaver AS Java. This technology stack is part of the SAP Solution Manager, which is a support and system management suite.

The SAP NetWeaver AS for Java technology supports the SAP Portal component, which may therefore be affected by this vulnerability and is typically exposed to the internet. Passive analysis of internet-facing applications indicates that a number of such applications are connected to the internet and could be affected by this vulnerability.

Description

On July 13, 2020 EST, SAP released the patch for a critical vulnerability, CVE-2020-6287, affecting its NetWeaver AS for Java component. This vulnerability can lead to compromise of vulnerable SAP installations, including the modification or extraction of highly sensitive information, as well as the disruption of critical business processes. A remote, unauthenticated attacker can exploit this vulnerability through an HTTP interface, which is typically exposed to end users and, in many cases, exposed to the internet.

Give Feedback

The vulnerability is introduced due to the lack of authentication in a web component of the SAP NetWeaver AS for Java allowing for several high-privileged activities on the SAP system.

Impact

If successfully exploited, a remote, unauthenticated attacker can obtain unrestricted access to SAP systems through the creation of high-privileged users and the execution of arbitrary operating system commands with the privileges of the SAP service user account (`<sid>adm`), which has unrestricted access to the SAP database and is able to perform application maintenance activities, such as shutting down federated SAP applications. The confidentiality, integrity, and availability of the data and processes hosted by the SAP application are at risk by this vulnerability.

Mitigations

CISA strongly recommends organizations review SAP Security Note #2934135 for more information and apply critical patches as soon as possible. CISA recommends prioritizing patching over application of individual mitigations. When patching, external facing systems should be urgently addressed, followed by internal systems.

Patched versions of the affected components are available at the SAP One Support Launchpad <https://launchpad.support.sap.com/>.

Give Feedback

Additional Recommendations

CISA encourages users and administrators of SAP products to:

- Scan SAP systems for all known vulnerabilities, such as missing security patches, dangerous system configurations, and vulnerabilities in SAP custom code.
- Apply missing security patches immediately and institutionalize security patching as part of a periodic process
- Ensure secure configuration of your SAP landscape
- Identify and analyze the security settings of SAP interfaces between systems and applications to understand risks posed by these trust relationships.

- Analyze systems for malicious or excessive user authorizations.
- Monitor systems for indicators of compromise resulting from the exploitation of vulnerabilities.
- Monitor systems for suspicious user behavior, including both privileged and non-privileged users.
- Apply threat intelligence on new vulnerabilities to improve the security posture against advanced targeted attacks.
- Define comprehensive security baselines for systems and continuously monitor for compliance violations and remediate detected deviations.

These recommendations apply to SAP systems in public, private, and hybrid cloud environments.

See the Onapsis report on the “RECON” SAP Vulnerability <https://www.onapsis.com/recon-sap-cyber-security-vulnerability> for more information.

ACKNOWLEDGEMENTS

SAP and Onapsis contributed to this Alert.

References

[1] Onapsis Threat Report <https://www.onapsis.com/recon-sap-cyber-security-vulnerability>
[2] CVE-2020-6287
[3] SAP Security Note <https://launchpad.support.sap.com/#/notes/2934135>
[4] SAP Trust Center <http://www.sap.com/security>
[5] SAP Monthly Security Patch Day Blog

Revisions

July, 13 2020: Initial Version

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov

Give Feedback

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </no-fear-act>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>