The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

DATE(S) ISSUED:
02/09/2022

SUBJECT: Multiple Vulnerabilities in SAP Products Could Allow for Remote Code Execution

OVERVIEW: Multiple vulnerabilities have been discovered in SAP products, the most severe of which (CVE-2022-22536) could allow for remote code execution. SAP is a software company which creates software to manage business operations and customer relations. Successful exploitation of the most severe of these vulnerabilities could allow an unauthenticated, remote attacker to execute code on the affected systems. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Applications configured to have fewer restrictions on the system could be less impacted than those who operate with elevated privileges.

THREAT INTELLIGENCE: There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- SAP Web Dispatcher, Versions - 7.49, 7.53, 7.77, 7.81, 7.85, 7.22EXT, 7.86, 7.87
- SAP Content Server, Version - 7.53
- SAP NetWeaver and ABAP Platform, Versions - KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49
- SAP Solution Manager (Diagnostics Root Cause Analysis Tools), Version – 720
- SAP NetWeaver AS ABAP (Workplace Server) and Java application Servers, Versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 787
- SAP ERP HCM (Portugal), Versions - 600, 604, 608
- SAP Business Objects Web Intelligence (BI Launchpad) , Version – 420
- SAP 3D Visual Enterprise Viewer , Version - 9.0
- SAP Adaptive Server Enterprise , Version - 16.0
- SAP S/4HANA (Supplier Factsheet and Enterprise Search for Business Partner, Supplier and Customer) , Versions - 104, 105, 106

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in SAP products, the most severe of which could allow for remote code execution. Details of these vulnerabilities are as follows:

- Request smuggling and request concatenation in SAP NetWeaver, SAP Content Server and SAP Web Dispatcher which could allow for remote code execution. (CVE-2022-22536)
- HTTP request smuggling vulnerability which could allow for remote code execution. (CVE-2022-22532)
- A memory leak in memory pipe management that could lead to denial of service. (CVE-2022-22533)
- SQL Injection vulnerability in SAP NetWeaver AS ABAP (Workplace Server). (CVE-2022-22540)
- Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver. (CVE-2022-22534)
- Missing Authorization check in SAP ERP HCM. (CVE-2022-22535)
- XSS vulnerability in SAP Business Objects Web Intelligence (BI Launchpad). (CVE-2022-22546)
- Improper Input Validation in SAP 3D Visual Enterprise Viewer. (CVE-2022-22537, CVE-2022-22539, CVE-2022-22538)
- Information Disclosure in SAP Adaptive Server Enterprise. (CVE-2022-22528)
- Information Disclosure vulnerability in SAP S/4HANA (Supplier Factsheet and Enterprise Search for Business Partner, Supplier and Customer). (CVE-2022-22542)
- Denial of service (DOS) in SAP NetWeaver Application Server for ABAP (Kernel) and ABAP Platform (Kernel). (CVE-2022-22543)

Successful exploitation of the most severe of these vulnerabilities could allow an authenticated, remote attacker to execute code on the affected systems. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Applications configured to have fewer restrictions on the system could be less impacted than those who operate with elevated privileges.

RECOMMENDATIONS:

*

The following actions should be taken:

- Apply appropriate updates provided by SAP to vulnerable systems, immediately after appropriate testing.
- Consider using the following tool created by Onapsis to scan your systems to see if they are vulnerable to CVE-2022-22536.
    - https://learn.cisecurity.org/e/799323/Onapsis-onapsis-icmad-scanner/qsj4h/258781276?h=dfh2aXkHM6SOfDYe3DZkqGdXNqVIipN2AjIS-vFF3kA
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding threats posed by hypertext links contained in emails or attachments, especially from un-trusted sources.

Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

SAP:
https://wiki.scn.sap.com/wiki/display/PSR/SAP+Security+Patch+Day+-+February+2022

Onapsis:https://onapsis.com/icmad-sap-cybersecurity-vulnerabilities?utm_campaign=2022-Q1-global-ICM-campaign-page&utm_medium=website&utm_source=third-party&utm_content=CISA-alerthttps://github.com/Onapsis/onapsis_icmad_scanner

Tenable:https://www.tenable.com/blog/cve-2022-22536-sap-patches-internet-communication-manager-advanced-desync-icmad

CVE:https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22528
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22532
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22534https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22535https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-

2022-22536
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22537
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22538
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22539https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22540
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22542
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22543https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22546