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
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
06/09/2021

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 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 Commerce, Versions – 1808, 1811, 1905, 2005, 2011
- SAP NetWeaver AS ABAP and ABAP Platform, Versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 804
- SAP NetWeaver AS for JAVA, Versions - 7.20, 7.30, 7.31, 7.40, 7.50
- SAP NetWeaver AS for ABAP (RFC Gateway), Versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73,7.77,7.81,7.82,7.83
- SAP NetWeaver ABAP Server and ABAP Platform (Enqueue Server), Versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73
- SAP NetWeaver ABAP Server and ABAP Platform (Dispatcher), Versions - KRNL32NUC - 7.22,7.22EXT, KRNL32UC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73,7.77,7.81,7.82,7.83
- SAP Business One, Version - 10.0
- SAP Manufacturing Execution, Versions - 15.1, 1.5.2, 15.3, 15.4

- SAP NetWeaver AS ABAP and ABAP Platform (SRM_RFC_SUBMIT_REPORT), Versions - 700, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755
- SAP NetWeaver AS for ABAP (Web Survey), Versions - 700, 702, 710, 711, 730, 731, 750, 750, 752, 75A, 75F
- SAP NetWeaver AS (Internet Graphics Server – Portwatcher), Versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81
- SAP Enable Now (SAP Workforce Performance Builder - Manager), Versions - 10.0, 1.0
- SAP NetWeaver AS ABAP, Versions - KRNL32NUC - 7.22,7.22EXT, KRNL32UC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73,7.77,7.81,7.82,7.83,7.84
- SAP NetWeaver AS for Java (UserAdmin), Versions - 7.11,7.20,7.30,7.31,7.40,7.50
- SAP NetWeaver Application Server ABAP (Applications based on Web Dynpro ABAP), Versions - SAP_UI – 750,752,753,754,755, SAP_BASIS – 702, 31
- SAP NetWeaver Application Server ABAP (Applications based on SAP GUI for HTML), Versions - KRNL64NUC - 7.49, KRNL64UC - 7.49,7.53, KERNEL - 7.49,7.53,7.77,7.81,7.84
- SAP Commerce Cloud, Version – 100
- SAP 3D Visual Enterprise Viewer, Version – 9
- SAP Fiori Apps 2.0 for Travel Management in SAP ERP, Version - 608

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

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:

- Remote Code Execution vulnerability in Source Rules that affects SAP Commerce (CVE-2021-27602)
- Improper Authentication in SAP NetWeaver ABAP Server and ABAP Platform (CVE-2021-27610)
- Missing XML Validation in SAP NetWeaver AS for JAVA (CVE-2021-27635)
- Multiple memory corruption vulnerabilities in SAP NetWeaver ABAP Server and ABAP Platform (CVE-2021-27606, CVE-2021-27629, CVE-2021-27630, CVE-2021-27631, CVE-2021-27632, CVE-2021-27597, CVE-2021-27633, CVE-2021-27634, CVE-2021-27607, CVE-2021-27628)
- Information Disclosure vulnerability in SAP Business One (CVE-2021-33662)
- Cross-Site Scripting (XSS) vulnerability in SAP Manufacturing Execution (CVE-2021-27615)
- Missing Authorization check in SAP NetWeaver AS ABAP and ABAP Platform (CVE-2021-21473)
- Cross-Site Scripting (XSS) vulnerability in SAP Netweaver AS for ABAP (Web Survey) (CVE-2021-21490)

- Multiple memory corruption vulnerabilities in SAP IGS (CVE-2021-27620, CVE-2021-27622, CVE-2021-27623, CVE-2021-27624, CVE-2021-27625, CVE-2021-27626, CVE-2021-27627)
- Information Disclosure in SAP Enable Now (SAP Workforce Performance Builder - Manager) (CVE-2021-27637)
- Plaintext command injection in SAP NetWeaver AS ABAP (CVE-2021-33663)
- Information Disclosure in SAP NetWeaver AS JAVA (UserAdmin Application) (CVE-2021-27621)
- Cross-Site Scripting (XSS) vulnerability within SAP NetWeaver AS ABAP (Applications based on Web Dynpro ABAP) (CVE-2021-33664)
- Cross-Site Scripting (XSS) vulnerability within SAP NetWeaver AS ABAP (Applications based on SAP GUI for HTML) (CVE-2021-33665)
- MIME Sniffing Vulnerability in SAP Commerce Cloud (CVE-2021-33666)
- Multiple improper input validation vulnerabilities in SAP 3D Visual Enterprise Viewer (CVE-2021-27638, CVE-2021-27639, CVE-2021-27640, CVE-2021-33659, CVE-2021-27642, CVE-2021-33661, CVE-2021-27641, CVE-2021-27643, CVE-2021-33660)
- Missing Authorization check in HCM Travel Management Fiori Apps V2 (CVE-2021-27605)

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.
- 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/pages/viewpage.action?pageId=578125999

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21473
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21490
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27597
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27602
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27605
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27606
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27607
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27610
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27615

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27620
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27621
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27622
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27623
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27624
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27625
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27626
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27627
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27628
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27629
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27630
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27631
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27632
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27633
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27634
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27635
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27637
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27638
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27639
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27640
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27641
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27642
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27643
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33659
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33660
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33661
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33662
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33663
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33664
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33665
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33666