

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

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<https://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

09/08/2020

SUBJECT:

Multiple Vulnerabilities in SAP Products Could Allow for Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in SAP products, the most severe of which could allow for arbitrary 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 Marketing (Mobile Channel Servlet), Versions - 130, 140, 150
- SAP NetWeaver (ABAP Server) and ABAP Platform, Versions - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755
- SAP NetWeaver AS ABAP (BSP Test Application), Versions - 700,701,702,730,731,740,750,751,752,753,754,755
- SAP NetWeaver (Knowledge Management), Versions - 7.30,7.31,7.40,7.50
- SAP Fiori (Launchpad), Versions - 750, 752, 753, 754, 755
- SAP Banking Services (Bank Analyzer), Version – 500
- SAP Commerce, Versions - 6.7, 1808, 1811, 1905, 2005
- SAP Business Objects Business Intelligence Platform (BI Workspace), Versions - 4.1, 4.2
- SAP Adaptive Server Enterprise, Versions - 15.7, 16.0
- S/4Hana; Version – 100

RISK:

Government:

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

Businesses:

- Large and medium business entities: **Medium**
- 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 arbitrary code execution. Details of the vulnerabilities are as follows:

- Access control vulnerability that affects SAP Marketing (CVE-2020-6320)
- Arbitrary code execution that affects SAP NetWeaver (CVE-2020-6318)
- Improper authorization checks that affect SAP Banking services (CVE-2020-6311)
- Session Fixation vulnerability that affects SAP Commerce (CVE-2020-6302)
- Cross-Site Scripting (XSS) vulnerability that affects SAP NetWeaver AS ABAP (CVE-2020-6324)
- Cross-Site Scripting (XSS) vulnerabilities that affects SAP NetWeaver AS Java (CVE-2020-6326, CVE-2020-6313)
- Cross-Site Scripting (XSS) vulnerability that affects SAP Fiori (CVE-2020-6283)
- Multiple vulnerabilities have been found in SAP BusinessObjects (CVE-2020-6312, CVE-2020-6288, CVE-2020-6325)
- Information disclosure vulnerability in SAP Adaptive Server Enterprise (CVE-2020-6317)

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.

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 the 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=557449700>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6288>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6283>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6326>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6324>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6325>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6320>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6318>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6317>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6313>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6312>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6311>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6302>

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<https://www.us-cert.gov/tlp/>