

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.

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

DATE(S) ISSUED:

07/13/2020

07/16/2020 - UPDATED

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 an unauthenticated, remote attacker to execute code on the affected systems. SAP is a company that 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.

July 16 – UPDATED THREAT INTELLIGENCE:

Proof of Concept exploits for CVE-2020-6287 and CVE-2020-6286 vulnerabilities were released on Github. Active scans for these vulnerabilities has been reported with the PoC likely utilized to compromise vulnerable SAP NetWeaver systems.

SYSTEMS AFFECTED:

- SAP NetWeaver AS JAVA (LM Configuration Wizard); Versions - 7.30, 7.31, 7.40, 7.50
- SAP Business Client, Version - 6.5
- SAP NetWeaver (XML Toolkit for JAVA); Versions - ENGINEAPI 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50
- SAP Disclosure Management; Version - 1.0
- SAP Business Objects Business Intelligence Platform (BI Launchpad); Version - 4.2
- SAP Business Objects Business Intelligence Platform (bipodata); Version - 4.2
- SAP NetWeaver AS JAVA (IIOP service) (SERVERCORE); Versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50

- SAP NetWeaver AS JAVA (IIOP service) (CORE-TOOLS); Versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50
- SAP Business Objects Business Intelligence Platform (BI Launchpad and CMC); Versions - 4.1, 4.2
- SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface) , Versions - 4.1, 4.2
- SAP NetWeaver (ABAP Server) and ABAP Platform; Versions - 731, 740, 750

RISK:

Government:

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

Businesses:

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

Home users: N/A

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in SAP products, the most severe of which could allow an unauthenticated, remote attacker to execute code on the affected systems. Details of the vulnerabilities are as follows:

- Multiple Vulnerabilities in SAP NetWeaver AS JAVA (LM Configuration Wizard) (CVE-2020-6286).
- Security updates for the browser control Google Chromium delivered with SAP Business Client
- Information Disclosure in SAP NetWeaver (XMLToolkit for Java) (CVE-2020-6285).
- Multiple vulnerabilities in SAP Disclosure Management (CVE-2020-6267).
- Cross-Site Scripting (XSS) vulnerability in SAP Business Objects Business Intelligence Platform(BI Launch pad) (CVE-2020-6281).
- Cross-Site Scripting (XSS) vulnerability in SAP Business Objects Business Intelligence Platform(Bipodata) (CVE-2020-6276).
- Server-Side Request Forgery in SAP NetWeaver AS JAVA (IIOP service) (CVE-2020-6282).
- Cross-Site Scripting (XSS) vulnerability in SAP Business Objects Business Intelligence Platform (BI Launchpad and CMC) (CVE-2020-6278).
- Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface) (CVE-2020-6222).
- Information Disclosure in SAP NetWeaver (ABAP Server) and ABAP Platform (CVE-2020-6280).

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=552599675>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6222>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6267>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6276>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6278>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6280>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6281>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6282>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6285>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6286>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6287>

July 16 - UPDATED REFERENCES:

<https://www.bleepingcomputer.com/news/security/poc-exploits-released-for-sap-recon-vulnerabilities-patch-now/>

TLP: WHITE

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

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