MINISTRY OF
HOME AFFAIRS
CAYMAN ISLANDS GOVERNMENT

National Cyber Awareness System:

TA16-132A: Exploitation of SAP Business Applications

05/11/2016 07:31 AM EDT

Original release date: May 11, 2016

Systems Affected

Outdated or misconfigured SAP systems

Overview

At least 36 organizations worldwide are affected by an SAP vulnerability [1]. Security researchers from Onapsis discovered indicators of exploitation against these organizations' SAP business applications.

The observed indicators relate to the abuse of the Invoker Servlet, a built-in functionality in SAP NetWeaver Application Server Java systems (SAP Java platforms). The Invoker Servlet contains a vulnerability that was patched by SAP in 2010. However, the vulnerability continues to affect outdated and misconfigured SAP systems.

Description

SAP systems running outdated or misconfigured software are exposed to increased risks of malicious attacks.

The Invoker Servlet vulnerability affects business applications running on SAP Java platforms.

SAP Java platforms are the base technology stack for many SAP business applications and technical components, including:

- SAP Enterprise Resource Planning (ERP),
- SAP Product Lifecycle Management (PLM),
- SAP Customer Relationship Management (CRM),
- SAP Supply Chain Management (SCM),
- SAP Supplier Relationship Management (SRM),
- SAP NetWeaver Business Warehouse (BW),
- SAP Business Intelligence (BI),
- SAP NetWeaver Mobile Infrastructure (MI),
- SAP Enterprise Portal (EP),
- SAP Process Integration (PI),

- SAP Exchange Infrastructure (XI),
- SAP Solution Manager (SolMan),
- SAP NetWeaver Development Infrastructure (NWDI),
- SAP Central Process Scheduling (CPS),
- SAP NetWeaver Composition Environment (CE),
- SAP NetWeaver Enterprise Search,
- SAP NetWeaver Identity Management (IdM), and
- SAP Governance, Risk & Control 5.x (GRC).

The vulnerability resides on the SAP application layer, so it is independent of the operating system and database application that support the SAP system.

Impact

Exploitation of the Invoker Servlet vulnerability gives unauthenticated remote attackers full access to affected SAP platforms, providing complete control of the business information and processes on these systems, as well as potential access to other systems.

Solution

In order to mitigate this vulnerability, US-CERT recommends users and administrators implement SAP Security Note 1445998 and disable the Invoker Servlet. For more mitigation details, please review the Onapsis threat report [1].

In addition, US-CERT encourages that users and administrators:

- Scan systems for all known vulnerabilities, such as missing security patches and dangerous system configurations.
- 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.

Note: The U.S. Government does not endorse or support any particular product or vendor.

References

- [1] Onapsis Threat Report: Wild Exploitation & Cyber-Attacks on SAP Business Applications
- [2] SAP: Invoker Servlet

Revision History

- May 11, 2016: Initial Release

Source: US-CERT