CYBER RISK ASSESSMENT

ONAPSIS

40,000+ ORGANIZATIONS USING SAP ARE AT RISK OF RECON VULNERABILITY

Successful Exploit Could Allow Unauthenticated Full System Access; Impact Business Operations and Regulatory Compliance

ASSESS YOUR SAP SYSTEMS TODAY

Are your mission-critical SAP systems and applications susceptible to RECON and other vulnerabilities? Onapsis offers a complimentary Cyber Risk Assessment to identify vulnerabilities, misconfigurations and other security issues that put your business at risk.

The results Onapsis delivers will help:

- Identify existing misconfigurations and vulnerabilities
- Prioritize and expedite remediation plans
- Reduce the overall attack surface
- Protect your mission-critical applications

Discovery and assessment is run remotely, takes less than two hours and does not require installation of software or access to production systems.

ERP SYSTEMS AND MISSION-CRITICAL APPLICATIONS AT RISK

A recent IDC survey of 430 IT decision makers titled, "ERP Security: The Reality of Business Application Protection" found that 64% of organizations have reported an ERP system—SAP and Oracle E-Business Suite—breach in the past 24 months. The research further suggests that these ERP systems are increasingly under attack for critical data. Among companies whose ERP systems have been breached in the last 24 months, the information compromised the most includes sales data (50%), customer personally identifiable information (41%), intellectual property (36%) and financial data (34%). Respondents ranked financial and sales data as the two most critical types of compromised data.

NEW RECON VULNERABILITY IN SAP

The SAP July 2020 Security Notes include a fix for a critical vulnerability—CVSS score of 10 out of 10—named RECON (Remotely Exploitable Code On NetWeaver). This is a very serious vulnerability affecting a default component present in every SAP application running the SAP NetWeaver Java technology stack. This technical component is used in many SAP business solutions, including SAP S/4HANA, SAP SCM, SAP CRM, SAP CRM, SAP Enterprise Portal, SAP Solution Manager (SolMan) and others putting more than 40,000 organizations using SAP at risk.

The RECON vulnerability is particularly dangerous because many of the affected solutions are often exposed to the internet to connect companies with business partners, employees and customers, which significantly reduces the complexity of a remote attack.

BUSINESS IMPACT OF EXPLOITS AGAINST RECON

If exploited, an unauthenticated attacker (no username or password required) can create a new SAP user with maximum privileges, bypassing all access and authorization controls (such as segregation of duties, identity management and GRC solutions) and gaining full control of SAP systems. This could allow them to perform many malicious activities, including the ability to modify financial records, view personally identifiable information (PII), corrupt data, delete or modify logs and traces and other actions that put essential business operations at risk. Because of the type of unrestricted access an attacker could obtain, this vulnerability may also constitute a deficiency in an enterprise's IT controls for regulatory mandates—potentially impacting financial (Sarbanes-Oxley) and privacy (GDPR) compliance.

For more information about the RECON vulnerability, read the Onapsis Threat Report at https://www.onapsis.com/recon-sap-cyber-security-vulnerability.