- Risk Management
- Compliance
- Privacy
- Supply Chain

- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security
- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response
- ICS/OT
- IoT Security

Home › Vulnerabilities

Nine Critical and High-Severity Vulnerabilities Patched in SAP Products

By Eduard Kovacs on August 11, 2021

German enterprise software giant SAP has released 19 new and updated security notes, including for nine new vulnerabilities that have been rated *critical* or *high severity*.

One of the critical vulnerabilities is CVE-2021-33698, an unrestricted file upload issue affecting SAP Business One. According to Onapsis, a company that specializes in protecting business-critical applications, the flaw can be exploited by an attacker to upload script files, which suggests that it can be exploited for arbitrary code execution.

The second critical security hole, identified as CVE-2021-33690, has been described as a server-side request forgery (SSRF) affecting NetWeaver Development Infrastructure. An attacker can exploit the vulnerability for proxy attacks by sending specially crafted queries, and if the targeted instance is exposed to the internet, a hacker can “completely compromise sensitive data residing on the server, and impact its availability.”

The third critical vulnerability, CVE-2021-33701, is a SQL injection in the SAP NZDT (Near Zero Downtime Technology) service used by S/4HANA and the DMIS mobile plug-in.

It’s worth noting that SAP assigns a “Hot News” severity rating to critical vulnerabilities.

The high-severity vulnerabilities patched by SAP include two cross-site scripting (XSS) flaws and an SSRF issue in NetWeaver Enterprise Portal. These vulnerabilities were discovered by researchers at Onapsis.

According to the security firm, the XSS flaws impact two of the portal's servlets and they allow an attacker to inject JavaScript code into the corresponding pages. The code is executed in the victim's browser when they access the compromised servlet.

As for the SSRF bug, it allows an unauthenticated attacker to make requests to internal or external servers by getting the targeted user to click on a malicious link.

Other vulnerabilities rated *high severity* include an authentication issue affecting all SAP systems accessed through a Web Dispatcher, a task hijacking issue in the Fiori Client mobile app for Android, and a missing authentication flaw in SAP Business One.

"With nine critical patches in total (considering patches with HotNews and High Priority as critical), SAP customers are facing the most noteworthy SAP Patch Day this year. The small group of SAP applications that are affected by a CVSS 9.9 vulnerability in 2021 is now extended with SAP Business One and SAP NetWeaver Development Infrastructure," Onapsis said in a blog post.

SAP customers should not neglect these patches. A study conducted earlier this year by SAP and Onapsis showed that threat actors often start targeting SAP application vulnerabilities within days after patches are made available.

Related: SAP Patches High-Severity Flaws in Business One, NetWeaver Products

Related: SAP Patches Critical Vulnerabilities in NetWeaver

Related: Another Critical Vulnerability Patched in SAP Commerce

Eduard Kovacs (@EduardKovacs) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia's security news reporter. Eduard holds a bachelor's degree in industrial informatics and a master's degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs:
Decryption Key for Ransomware Delivered via Kaseya Attack Made Public
OwnBackup Raises $240 Million at $3.35 Billion Valuation
Intel Patches High-Severity Flaws in NUC 9 Extreme Laptops, Ethernet Linux Drivers
Nine Critical and High-Severity Vulnerabilities Patched in SAP Products
Firefox 91 Brings New Privacy, Security Improvements

Tags:
NEWS & INDUSTRY Vulnerabilities