APPSIAN   SAP SECURITY BRIEF

SAP RECON Vulnerability Puts Thousands of ERP Customers at Risk

Rajesh Rengarethinam • VP of Engineering (SAP)

A critical SAP vulnerability (CVE-2020-6287 or RECON) was recently discovered by Onapsis that gives attackers TOTAL control of vulnerable business applications. The RECON vulnerability allows hackers to penetrate SAP systems and create new users with administrative privileges, allowing them to manage (read/modify/delete) every record/file/report in the system.

The RECON bug is one of those rare vulnerabilities that received a maximum of 10 out of 10 rating on the CVSSv3 vulnerability severity scale, so it is crucial that organizations move quickly to apply patches.

Remote and unauthenticated attackers can exploit the vulnerability to create a new SAP admin user, bypassing access and authorization controls and gaining full control of the SAP system. Exploitation will impact the confidentiality, integrity, and availability of SAP applications.

With an admin-level user account at their disposal, an attacker can:

- Steal personal identifiable information (PII) from employees, customers, and suppliers
- Read, modify or delete financial records
- Change banking details (account number, IBAN number, etc.)
- Administer purchasing processes
- Disrupt the operation of the system by corrupting data or shutting it down completely
- Perform unrestricted actions through operating system command execution
- Delete or modify traces, logs and other files

The RECON Attack Path

The RECON vulnerability is easy to exploit and resides in the LM Configuration Wizard component of the SAP NetWeaver Application Server (AS) JAVA. The LM Configuration Wizard of SAP NetWeaver (AS) JAVA does not perform an authentication check, allowing an attacker without prior authentication to execute configuration tasks to perform critical actions against the SAP Java system, including the ability to create an administrative user. This compromises the Confidentiality, Integrity, and Availability of the system.

The vulnerability not only compromises the security of the NetWeaver Java applications but can also be used to exfiltrate credentials to an ABAP system through the ABAP secure storage and potentially lead to the exposure of ERP data-sensitive PII and financial information.

SAP Guidance: Apply the Patch or Enable a Workaround

The critical nature of this vulnerability caused the Cybersecurity and Infrastructure Security Agency (CISA) to strongly recommend organizations immediately apply patches, as noted in SAP Security Note #2934135.

If you cannot apply the patch, then at least disable the tc~lm~ctc~cul~startup_app application, as described in SAP Security Note 2939665. Note 2939665 is a workaround and a defense-in-depth, but not a solution.

Further Risk Mitigation Measures

Being up to date on the patches will help mitigate the vulnerability. Still, because of the number of security patches released in recent years, several customers are behind on these as the application of these patches requires downtime of the production systems. Moreover, the time to apply the patches depends on the complexity and the components involved. It can require a significant amount of time and effort, especially if the systems are a couple of patches behind.

All this ends up increasing the risk and the timeframe for which the systems are exposed. Having application security in the form of multi-factor authentication or additional policy-based controls and logging will help mitigate the risks and control sensitive data exposure in mission-critical systems.

Talk to the SAP Security Experts at Appsian today to discuss how your organization can address the risks posed by RECON and other vulnerabilities.