www.pwc.com/cybersecurity

The right response to the SAP security flaw

Using an old vulnerability to help build new cybersecurity capabilities

A recent alert from the US Computer Emergency Readiness Team (US-CERT) warned that cybercriminals are targeting SAP business applications using a security defect that was patched in 2010. The fact that businesses remain vulnerable to a bug that was resolved five years ago should serve as a wake-up call for organizations to assess and update security practices for their SAP systems.

The flaw represents a major vulnerability for SAP customers because it can enable cybercriminals to remotely control business operations and processes, as well as access other applications and data from within the SAP environment.[1] In other words, the vulnerability offers up a free pass into an organization's most important applications and information.

US-CERT said indicators of exploitation have been discovered, affecting at least 36 organizations worldwide since 2013. Adding to the urgency. Individuals have publically discussed exploit techniques and vulnerable companies in Chinese-language digital security forums for the past several years, according to Onapsis, a Boston-based SAP cybersecurity firm, that detailed the vulnerability.[2]

Given the massive amount of critical data stored on SAP applications—SAP says its customers comprise 87% of the Forbes Global 2000 Companies—the impacts are potentially enormous and costly.[3] Financial losses due to theft of financial, human resources, business strategy, employee and customer, R&D, intellectual property, and supplier information could be significant. What's more, attackers could use the vulnerability to shut down essential business and manufacturing services, incurring significant financial, operational and reputational damages.

Separate, but insecure, systems

The SAP defect may be news in the C-suite but, as noted, the flaw was patched years ago. So why do businesses remain vulnerable? In a word, complexity. Due to the intricate demands of SAP applications, security is typically managed by application specialists rather than enterprise security teams. As a result, SAP security maintenance is siloed and the enterprise cybersecurity team often lacks visibility into the SAP environment.

Complicating matters is the fact that administrators typically manage SAP software as an internal system and tend to focus on application-specific controls. In doing so, they may fail to properly implement processes and technologies to help guard against external Internet-facing attacks that the vulnerability makes possible.

Patching, in particular, remains an enormous challenge. SAP applications often underpin an organization's entire technology ecosystem and comprise a complex network of interconnected applications that are complicated to update. It may be difficult to determine what patches are critical and what additional configurations will be required after an SAP update is implemented. As a result, SAP patches may require an investment in time and resources that businesses can be reluctant to undertake.

---

[1] US-CERT, *Alert (TA16-132A), Exploitation of SAP Business Applications*, May 11, 2016

[2] Onapsis, *Threat Report: The Tip of the Iceberg: Wild Exploitation and Cyber-Attacks on SAP Business Systems*, May 2016

[3] SAP, *SAP: Run Simple–The World's Largest Provider of Enterprise Application Software*, accessed May 12, 2016

Another concern is that SAP updates can potentially destabilize business systems and put information at risk. Consequently, many organizations prioritize the availability and stability of business-critical applications, and relegate SAP patches to the back burners of maintenance initiatives.

Taking action to protect your business

No specific breach, as yet, has been linked to the SAP defect. Nonetheless, businesses should review their landscape of SAP systems to quantify exposure and, if necessary, disable the Invoker Servlet for each affected application (see sidebar).

Ultimately, the flaw may be more instructive than destructive in that it provides an opportunity to initiate a discussion about aligning SAP security with enterprise cybersecurity practices.

Putting security at the fore of SAP application management will likely require an integrated, risk-based approach. SAP security should no longer be pigeonholed as the responsibility of application specialists: rather, it should be aligned with overall cybersecurity strategy, processes and people skills.

The first steps in developing a risk-based approach will be to understand, classify and prioritize critical assets and threats to the SAP environment. This assessment should take into account external risks unique to the business and the industry in which it operates, as well as include a full quantification of the operational impact and financial costs of these risks. Businesses should also identify critical operations within SAP that could be impacted, such as manufacturing and production lines.

Next, organizations should standardize SAP application management with overall cybersecurity strategy to improve processes such as regular patching, authentication, real-time monitoring and intrusion detection. Continuous monitoring of privileged and non-privileged users should be adopted as a means to detect suspicious behavior and insider risks related to SAP applications. It's also important to conduct an SAP-specific assessment of processes, roles and technologies to identify potential vulnerabilities. As with other enterprise systems, it will be necessary to carefully assess the security settings of SAP interfaces between systems and applications, including all cloud-based services and data analytics solutions. An effective SAP security strategy should also include a cross-functional incident-response plan, one that is aligned with enterprise incident-response management.

Finally, businesses should extend the enterprise culture of security to include SAP managers and users. Doing so means that SAP is no longer viewed as a separate business suite with discrete cybersecurity practices and practitioners; it must be brought into the fold of overall enterprise security.

The power of PwC threat intelligence

Checking for exposure to the SAP vulnerability will likely be a relatively straightforward initiative for most information security departments. Determining whether the business has been hacked as a result of the defect, however, will require expertise and an arsenal of threat-detection and incident-response capabilities.

That's where PwC can help. Our team of SAP specialists has deep experience designing, implementing and running cybersecurity programs for SAP systems. PwC's proprietary threat-detection tools and research teams provide augmented abilities to detect and respond to intricate risks on complex systems like SAP. In addition, our capabilities are informed by a proprietary Threat Intelligence Fusion Center and Advanced Security Operations Centers, as well as real-time information culled from a wide range of open and closed commercial sources.

Businesses that lack these capabilities may be unable to effectively investigate and manage SAP vulnerabilities. What's more, the complexity of SAP systems often requires that businesses seek the assistance of experienced third parties to develop and implement an integrated strategy.

Now's a good time to start a conversation about SAP security with your executive and cybersecurity teams—and with a third party, if necessary.

How to detect and remediate the SAP bug

The SAP vulnerability is related to the SAP Java platform, a technology stack that business executives may not recognize as being part of their implementation. Specifically, the bug results from abuse of the Invoker Servlet, a built-in functionality in SAP NetWeaver Application Server Java systems, *according to US-CERT*.

The first step in investigating impact will be to determine if your company employs any of the affected SAP business systems (see below). Businesses that use one of these 18 applications should implement SAP Security Note *1445998* and disable the Invoker Servlet for each affected SAP system.

Potentially impacted SAP systems include:

- 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).

Contacts

To have a deeper discussion about the SAP business application vulnerability, please contact:

Scott A. Osterman

Partner
scott.a.osterman@pwc.com
(312) 298-5614

Peter Hobson

Director
peter.m.hobson@pwc.com
(646) 471-0203

Jonathan Wellner

Director
jonathan.m.wellner@pwc.com
(267) 330-2097