ONAPSIS

SAPSA

Zero-Day on SAP Netweaver: Lessons from CVE-2025-21324

Ernest Gutiérrez

November 2025

Our Onapsis Research Labs Are *The* World's SAP Security Experts

Trusted and Continuously Consulted by Government Security Agencies and the Market at Large

16+ Years

In Existence as the Most Trusted SAP Threat Research Group in the World

85+ Years

Combined of SAP and CyberSec Experience Across the Team

CISA | BSI | U.S. Department of Homeland Security

SAP **Product Security Response Team**

We Find More Vulnerabilities:

1,000+

zero-day vulnerabilities in business-critical applications

We're Who Govt Agencies Call:

6

US CISA critical alerts based on Onapsis research

We Have More Expertise:

10,000+

SAP vulnerabilities and attacks In our threat knowledgebase

RSA Conference | DEFCON | EKOPARTY | black hat | LEHACK | TROOPERS

Featured In CNBC | WSJ | FORTUNE | REUTERS | Forbes

Risk in SAP Applications Is Business Risk

RISK = **PROBABILITY** × **IMPACT**

- Dozens of known threat actors targeting SAP Applications, of all types.
- Automated and manual exploitation of SAP Vulnerabilities.
- Ransomware and malware with knowledge of SAP applications
- Cloud, on premises, and expanded attack surface

<3 hrs NEW SYSTEM ONLINE TO BEING EXPLOITED

<72 hrs SAP PATCH RELEASE TO EXPLOITATION

(*) https://onapsis.com/active-cyberattacks-business-critical-sap-applications

- Impact has always been critical to the business
- Known Incidents measured in Millions and also led to bankruptcy.
- Business processes are supported by SAP applications

92% of the Global 2000 use SAP or Oracle (1)

87% of the world's revenue touches these systems (2)

(1)https://www.sap.com/corporate/en/company.html?pdf-asset=4666ecdd-b67c-0010-82c7-eda71af511fa&page=1

(2)https://www.sap.com/documents/2017/04/4666ecdd-b67c-0010-82c7-eda71af511fa.html#page=1

ONAPSIS

Most Notable Vulnerabilities in 2025

Deserialization Vulnerabilities

The Numbers

- 8 Total Deserialization Vulnerabilities in 2025
- 7 Critical (CVSS ≥ 9.0) = 87.5% critical rate
- 3 with CVSS 10.0 (maximum severity)
- All 8 are HTTP exploitable
- All discovered/analyzed by Onapsis Research Labs

What is Deserialization?

The Risk: Applications that deserialize (reconstruct) untrusted data from users can be tricked into executing malicious code.

Why It's Critical:

- Often leads to Remote Code Execution (RCE)
- Frequently requires no or low authentication
- Can bypass traditional security controls

🔴 CVSS 10.0 - Zero Authentication Required

CVE-2025-31324 | SAP Note 3594142 | May 2025
Component: Visual Composer Development Server
Impact: Unauthenticated file upload → Full compromise

CVE-2025-30012 | SAP Note 3578900 | July 2025
Component: SRM Live Auction Cockpit
Impact: Unauthenticated RCE as SAP Administrator

CVE-2025-42944 | SAP Note 3660659 | November 2025
Component: NetWeaver AS Java (Core)
Impact: Unauthenticated RCE on Java stack

🟠 CVSS 9.1 - Privileged User Required

CVE-2025-42999 | Note 3604119 | Visual Composer
Risk: Root cause of CVE-2025-31324 - Attack reconstruction

CVE-2025-42964 | Note 3621236 | Enterprise Portal Content Directory
Risk: Gateway to entire SAP landscape

CVE-2025-42963 | Note 3621771 | NetWeaver Log Viewer
Risk: Weaponizes security monitoring

CVE-2025-42980 | Note 3620498 | Federated Portal Network
Risk: Multi-system portal compromise

CVE-2025-42966 | Note 3610892 | XML Data Archiving Service
Risk: Data management compromise

What is CVE-2025-31324

SAP Security Note

3594142 - [CVE-2025-31324] Missing Authorization check in SAP NetWeaver (Visual Composer development server)

Component: EP-VC-INF (Enterprise Portal > Visual Composer > Visual Composer Infrastructure), Version: 19, Released On: 13.05.2025

Symptom

SAP NetWeaver Visual Composer Metadata Uploader is not protected with a proper authorization, allowing unauthenticated agent to upload potentially malicious executable binaries that could severely harm the host system. This could significantly affect the confidentiality, integrity, and availability of the targeted system.

Recently Released Exploit for **CVE-2025-31324**

August 15th

Released on Telegram, by "*Scattered LAPSUS$ Hunters – ShinyHunters*"

Fully functional exploit

- Supporting both modes, direct command execution as well as webshell deployment
- Supporting the two latest versions of Netweaver: 7.50 and 7.40

Sophisticated Post-Exploitation

Deploying remote access tools like "Sakura", combining it with the theft of SAP credentials, pointing to a focused objective: long-term, persistent access to the organization's most critical systems.

Custom Tooling

Use of custom, more advanced webshells with features like encryption and password protection.

Targeting SAP-Specific Assets

Focus on gathering sensitive information like SAP-specific password stores, shows attackers:

- Know what these files are.
- Understand their value for lateral movement and deeper compromise within the SAP landscape.
- Know the specific locations or commands to find them.

ONAPSIS

Timeline

The SAP Zero-Day Wake Up Call: 500+ Companies Compromised

DARKREADING

Critical SAP NetWeaver Vuln Faces Barrage of Cyberattacks

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Known Exploited Vulnerabilities Catalog

CVE-2025-31324

SAP NetWeaver Unrestricted File Upload Vulnerability: *SAP NetWeaver Visual Composer*

CYBERSCOOP

THREATS

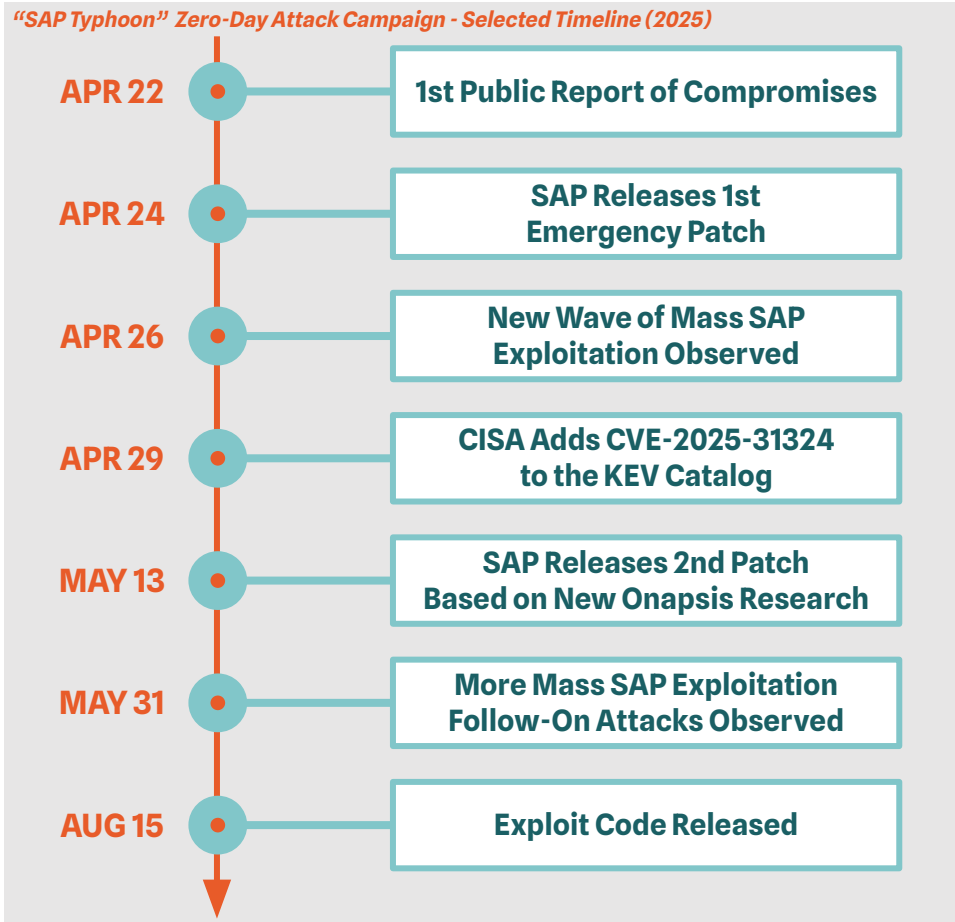
SAP cyberattack widens, drawing Salt Typhoon and Volt Typhoon comparisons

sky news • Watch Live

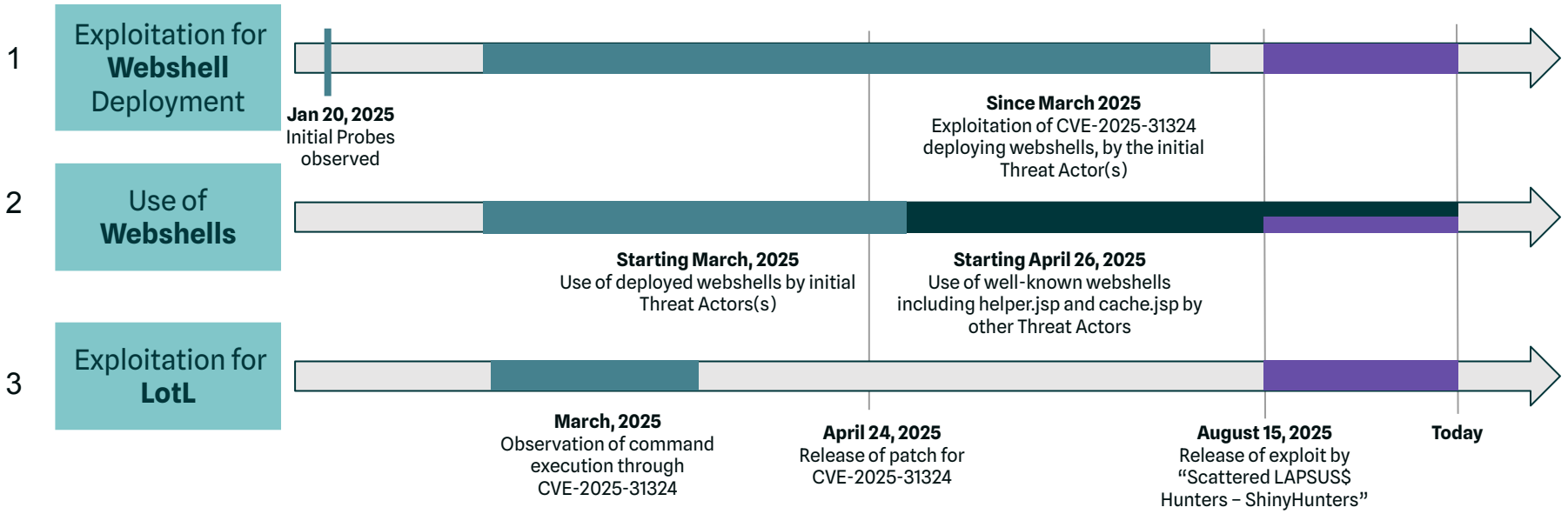
'China-based' hack targets UK companies in 'critical national security threat', says analyst

gbhackers.

Qilin Exploits SAP Zero-Day Vulnerability Weeks Ahead of Public Disclosure



Timeline for CVE-2025-31324



0-Day Threat Actor(s), suspected to be linked to Russian-Ransomware groups

Post 0-Day Threat Actor(s), mostly suspected to be linked to China-Nexus

Massive use of newly available exploit. Linked to various actors.

CVE-2025-31324 – Facts and Implications

- Sophisticated and Orchestrated Global attacks, in different waves, performed by different Threat Actor groups (with enough SAP knowledge, capabilities and resources to perform such activities). Latest public exploit from August makes exploitation possible for anyone.

- Huge economic impact (operations shut down, loss of revenue, reputational damage), including **Supply Chain & 3p context**.

CVE-2025-31324 – Facts and Implications

- Compliance penalties.
- Insurances*: Companies will have to **prove** that they really did enough to prevent the incident, otherwise they won't we covered...

* source:
https://www.insurancebusinessmag.com/uk/news/cyber/jlr-cyber-incident-tests-insurers-appetite-for-operational-risk-as-scattered-spider-surfaces-again-548432.aspx

And The Onapsis Platform: Application Security & Compliance Technology

Powered by Onapsis Research, Used By Market Leaders, and Fully Endorsed by SAP

ONAPSIS RESEARCH LABS — Technology Powered by the Deep Research and Global Threat Intelligence from the **Onapsis Research Labs**

SAP® Endorsed App
Premium Certified

ONAPSIS PLATFORM

16+ Years of SAP Security Data and Best Practices + AI + Automation

CONTROL
SAP Code Security Testing & DevSecOps

ASSESS
SAP App Vulnerability Management

DEFEND
SAP Application Security Monitoring

UNIFIED SAP APPLICATION ATTACK SURFACE MANAGEMENT

SAP | RISE WITH SAP | SAP BTP | On Premises | Hybrid | Cloud | SAP SuccessFactors

ONAPSIS

Final Takeaways

SAP Cybersecurity Vulnerabilities: A Different Type of Risk

Unauthenticated Compromise

- Attackers may not need a user, or a low privileged one
- Full Admin privileges
- Internal and/or external
- Bypasses existing SAP SoD & access controls
- Potentially leaves no trace of activity in standard SAP audit logs

Malicious / Unauthorized Business Activity

- Modify financial records
- Deploy ransomware
- View Personally Identifiable Information (PII)
- Corrupt Business Data
- Delete or modify logs, traces, and other actions that jeopardize essential Business operations

Deficiency in IT Controls for Regulatory Mandates

- Corporate liability for corrupted / modified Data
- Exfiltration of sensitive Data
- Exfiltration of financial Data
- Exposure of PII

Vulnerable and/or compromised systems may be under the scope of ie SOX, GDPR, NIS2, DORA, HIPAA, etc.

Protecting against these vulnerabilities is the Customer's responsibility in RISE with SAP / Cloud ERP Private, hybrid and on-prem SAP applications.

$1.2B+ in Quarterly Earnings Losses, $260M Direct Cyber Costs Due to SAP Exploitation and Data Breach at Jaguar Land Rover

- Jaguar Land Rover (JLR) disclosed cyber incident on September 2nd, 2025
- "ShinyHunters" claimed responsibility, stating they **gained access exploiting the *same* SAP vulnerability for which they released a public exploit in August 2025 (CVE-2025-31324)**
- Manufacturing operations were shutdown for 6+ weeks, 30,000+ employees furloughed.
- Substantial downstream effects on UK auto supply chain ecosystem, incl. bankruptcies, government intervention, job losses, and more
- **Q2 (Jul-Sep) performance *significantly affected* by the SAP cyber incident:**
  - **– $1.2B Q2 earnings shortfall, YoY**
  - **– $2.1B Q2 revenue drop, YoY**
  - **– $260M in direct, one-off cyber costs**

The claim was made on a Telegram messenger group, where a user linked to the hackers posted a screenshot of what appeared to show JLR's internal system.

A member of the group told The Telegraph that a well-known flaw in SAP Netweaver - third-party software used by JLR - was exploited to access the data.

https://www.thetimes.com/article/6ef32862-583a-43be-a987-40334142c025?shareToken=765bdbbf2bd075b773ced5da241b4bd0

ONAPSIS

SAP® Endorsed App
Premium Certified

Thank You!

Ernest Gutiérrez Roca
egutierrez@onapsis.com