Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00664-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	20 de junio de 2022
Última revisión	20 de junio de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información sobre nuevas vulnerabilidades en productos SAP.

Vulnerabilidades

CVE-2022-27668
CVE-2022-31590
CVE-2022-29611
CVE-2022-29618
CVE-2022-29612
CVE-2022-31589
CVE-2022-31595
CVE-2022-29614
CVE-2022-29615
CVE-2022-31594

Impacto

Vulnerabilidades de riesgo crítico:

CVE-2022-27668: Control de acceso inapropiado relacionado con el proxy SAProuter en NetWeaver y la plataforma ABAP.

Productos afectados

SAP NetWeaver y ABAP Platform, Versions -KERNEL 7.49, 7.77, 7.81, 7.85, 7.86, 7.87, 7.88, KRNL64NUC 7.49, KRNL64UC 7.49, SAP_ROUTER 7.53, 7.22
SAP PowerDesigner Proxy 16.7, Versions -16.7High7.8
SAP NetWeaver Application Server for ABAP and ABAP Platform,Version -700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 787, 788
SAP 3D Visual Enterprise Viewer, Version -9.0
SAP NetWeaver Development Infrastructure (Design Time Repository), Versions -7.30, 7.31, 7.40, 7.50

SAP NetWeaver, ABAP Platform and SAP Host Agent, Versions -KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, 7.88, 8.04, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53, 8.04, SAPHOSTAGENT 7.22
SAPERP, localization forCEEcountries, Versions -C-CEE110_600, 110_602, 110_603, 110_604, 110_700
SAP Financials, Versions -SAP_FIN 618, 720
SAP S/4Hana Core, Versions -S4CORE 100, 101, 102, 103, 104, 105, 106, 107, 108
SAP Adaptive Server Enterprise (ASE), Versions -KERNEL 7.22, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53
SAP NetWeaverASABAP,ASJava, ABAP Platform and HANA Database, Versions -KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, 7.88, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53, SAPHOSTAGENT 7.2
SAP NetWeaver Developer Studio (NWDS), Versions -7.50
SAP Adaptive Server Enterprise (ASE), Versions -KERNEL 7.22, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53Low3.2

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=10
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27668
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31590
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29611
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29618
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29612
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31589
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31595
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29614
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29615
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31594