Alerta de seguridad cibernética	9VSA21-00429-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de abril de 2021
Última revisión	23 de abril de 2021

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 equipo CSIRT. 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 varias vulnerabilidades en productos de Oracle, informadas por la compañía en su entrega de parches de abril.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2020-24750
CVE-2020-11979
CVE-2020-5421
CVE-2020-13954
CVE-2020-13871
CVE-2020-24750
CVE-2020-28052
CVE-2020-11612
CVE-2019-0228
CVE-2019-3900
CVE-2020-17527
CVE-2020-25649
CVE-2020-11987
CVE-2021-22112
CVE-2019-10086
CVE-2020-11987
CVE-2020-28052
CVE-2020-10188
CVE-2020-24750
CVE-2020-8203
CVE-2020-1971
CVE-2020-27218
CVE-2020-8203
CVE-2020-17521
CVE-2020-11022
CVE-2019-12423
CVE-2020-1927
CVE-2020-27193
CVE-2020-11022

Impactos

Entre las vulnerabilidades consideradas por Oracle como de riesgo alto están las siguientes:

CVE-2020-24750: Una vulnerabilidad permite a un atacante no autenticado ejecutar código arbitrario.

CVE-2020-13871: Esta vulnerabilidad existe debido a un error de uso de memoria después de ser liberada. Su explotación permite ejecutar código arbitrario en el sistema objetivo.

CVE-2020-10188: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo.

CVE-2020-24750: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo.

CVE-2019-3900: Esta vulnerabilidad permite a un atacante remoto realizar un ataque de denegación de servicio (DoS).

Productos Afectados

Oracle Communications Calendar Server: 8.0
Oracle Communications Unified Inventory Management: 7.3.4, 7.3.5, 7.4.0, 7.4.1.
Oracle Communications Design Studio: 7.4.2.
Oracle Communications Messaging Server: 8.1.
Oracle Communications Performance Intelligence Center Software: 10.4.0.3
Oracle Communications Performance Intelligence Center Software: 10.4.0.2
Oracle Communications Interactive Session Recorder: 6.3, 6.4
Oracle Communications Application Session Controller: 3.9m0p3
Oracle Communications MetaSolv Solution: 6.3.0, 6.3.1
Oracle Communications Contacts Server: 8.0
Oracle Communications Session Router: cz8.2, cz8.3, cz8.4
Oracle Communications Session Border Controller: cz8.2, cz8.3, cz8.4
Oracle Enterprise Communications Broker: PCz3.1, PCz3.2, PCZ3.3
Oracle Enterprise Session Border Controller: cz8.2, cz8.3, cz8.4
Oracle Communications Subscriber-Aware Load Balancer: cz8.2, cz8.3, cz8.4
Oracle Communications Converged Application Server - Service Controller: 6.2
Oracle Communications Services Gatekeeper: 6.0, 6.1, 7.0
Oracle Commerce Guided Search: 11.3.2
Oracle Commerce Merchandising: 11.3.0, 11.3.1, 11.3.2
Oracle SD-WAN Edge: 8.2, 9.0.
Oracle SD-WAN Aware: 8.2

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor cuando estén disponibles.

Enlaces

https://www.oracle.com/security-alerts/cpuapr2021.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24750
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11979

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5421
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13954
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13871
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24750
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28052
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11612
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0228
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-3900
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17527
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25649
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11987
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22112
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10086
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11987
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28052
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10188
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24750
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8203
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1971
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27218
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8203
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17521
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12423
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1927
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27193
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11022

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.04.23 20:05:58 -04'00'