Basque CyberSecurity Centre

Vulnerabilidades en servidores de Nvidia

BCSC-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Aviso de seguridad

Nvidia ha publicado una actualización de seguridad de firmware para servidores NVIDIA DGX-2, servidores DGX A100 y DGX Station A100. La severidad de las vulnerabilidades tratadas varía entre alta y moderada y los identificadores de las mismas son CVE-2022-42274, CVE-2022-42280, CVE-2022-42282, CVE-2022-42283, CVE-2022-42287, CVE-2023-0200, CVE-2023-0201, CVE-2022-42286, CVE-2022-42289, CVE-2022-42290, CVE-2023-0207, CVE-2023-0202, CVE-2023-0206.

Adicionalmente se corrigen 3 vulnerabilidades, 1 crítica CVE-2022-40259 y 2 altas CVE-2022-40242, CVE-2022-2827, que afectan a algunos controladores de administración de la placa base AMI MegaRAC SP-X.

Por último, se incluyen 8 vulnerabilidades que afectan a procesadores Intel, de las cuales 4 tienen una severidad alta y cuyos identificadores son CVE-2020-12357, CVE-2020-8670, CVE-2020-8700, CVE-2020-12359.

Estos fallos pueden conducir a condiciones de ejecución de código, de denegación de servicio, escalada de privilegios, pérdida de integridad de los datos, divulgación de información y/o manipulación de datos.

2. Recursos afectados

- Servidores NVIDIA DGX-2.
- Servidores DGX A100.
- DGX Station A100.
- Placa base AMI MegaRAC SP-X.

3. Análisis técnico

Los detalles de las vulnerabilidades más relevantes corregidas en esta actuañización son los siguientes:

CVE-2022-42274: vulnerabilidad en el controlador de IPMI en NVIDIA BMC donde un atacante con los privilegios necesarios puede provocar un desbordamiento de búfer, lo que podría conducir a condiciones de denegación de servicio o ejecución de código.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.8

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: Local
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-42280: vulnerabilidad en el controlador de autenticación REST de SPX en NVIDIA BMC, donde un atacante no autorizado puede explotar un cruce de ruta, lo que puede conducir a la omisión de la autenticación.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.1

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

- **Vector de ataque**: Local
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad:** Ninguna

CVE-2022-42289: vulnerabilidad en SPX REST API dentro del componente NVIDIA BMC, donde un atacante autorizado puede inyectar comandos de shell arbitrarios, lo que puede provocar la ejecución de código, denegación de servicio, divulgación de información y manipulación de datos.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.2

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos:** Altos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-42290: vulnerabilidad en SPX REST API en NVIDIA BMC, donde un atacante autorizado puede inyectar comandos de shell arbitrarios, lo que puede provocar la ejecución de código, denegación de servicio, divulgación de información y manipulación de datos.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.2

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos:** Altos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-0200: vulnerabilidad en OFBD en NVIDIA DGX-2, en la que un usuario con altos privilegios y un heap precondicionado puede provocar un acceso más allá del final de un búfer, lo que puede conducir a la ejecución de código, aumento de privilegios, denegación de servicio y divulgación de información.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.5

CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque**: Local
- **Complejidad del ataque**: Alta
- **Privilegios requeridos:** Altos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**

- **Disponibilidad: Alta**

CVE-2023-0202: vulnerabilidad en NVIDIA DGX A100 SBIOS en la que un atacante puede modificar la memoria arbitraria de SMRAM al explotar las API GenericSio y LegacySmmSredir SMM. Una explotación exitosa de esta vulnerabilidad puede conducir a la denegación de servicio, aumento de privilegios y divulgación de información.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.5

CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque**: Local
- **Complejidad del ataque**: Alta
- **Privilegios requeridos:** Altos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-0206: vulnerabilidad en NVIDIA DGX A100 SBIOS en la que un atacante puede modificar la memoria arbitraria de SMRAM explotando la API NVME SMM. Una explotación exitosa de esta vulnerabilidad puede conducir a la denegación de servicio, aumento de privilegios y divulgación de información.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.5

CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque**: Local
- **Complejidad del ataque**: Alta
- **Privilegios requeridos:** Altos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-0207: vulnerabilidad en NVIDIA DGX-2 SBIOS donde un atacante puede modificar la variable NVRAM ServerSetup en tiempo de ejecución mediante la ejecución de código privilegiado. Una explotación exitosa de esta vulnerabilidad puede conducir a la denegación de servicio.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.5

CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque**: Local
- **Complejidad del ataque**: Alta
- **Privilegios requeridos:** Altos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-40259: vulnerabilidad de credenciales predeterminadas en MegaRAC.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.3

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: Alta
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: Requerida
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-40242: vulnerabilidad de credenciales predeterminadas en MegaRAC.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.5

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad:** Ninguna
- **Disponibilidad:** Ninguna

CVE-2022-2827: vulnerabilidad de credenciales predeterminadas en MegaRAC.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.5

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad:** Ninguna
- **Disponibilidad:** Ninguna

4. Mitigación / Solución

Para la mitigación de estas vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

En el caso de este aviso de seguridad, Nvidia ha publicado las actualizaciones de firmware correspondientes a través de su Portal de Soporte Empresarial accesible desde el propio aviso.

5. Referencias Adicionales

- Actualización de seguridad.
- CVE-2022-42274, CVE-2022-42280, CVE-2022-42282, CVE-2022-42283, CVE-2022-42287, CVE-2023-0200, CVE-2023-0201, CVE-2022-42286, CVE-2022-42289, CVE-2022-42290, CVE-2023-0207, CVE-2023-0202, CVE-2023-0206.
- CVE-2022-40259, CVE-2022-40242, CVE-2022-2827.
- CVE-2020-12357, CVE-2020-8670, CVE-2020-8700, CVE-2020-12359.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA