Nro. Alerta:	EC-2022-050	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	18-marzo-2022	**Vulnerabilidad presente en tres equipos de marca NETGEAR puede ocasionar inyección de código remoto**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Inyección de código remoto
Nivel de riesgo: Alta

II. ALERTA

Una vulnerabilidad de desbordamiento de búfer en el servicio UPnP presente en hardware NETGEAR, en lo modelos EX6100 v1, CAX80 v2.1.2.6 y DC112A v1.0.0.62, puede conducir a la ejecución de código arbitrario sin autenticación.

Figura 1. Logotipo Netgear

III. INTRODUCCIÓN

La Empresa fabricante de equipos de red, con una amplia variedad de productos tanto a nivel doméstico como a nivel empresarial y ampliamente difundido a nivel global; presenta una vulnerabilidad del componente UPnP Service.

El CVE asignado para esta vulnerabilidad es CVE-2022-24655 siendo los productos afectados:

- Netgear EX6100
- Netgear CAX80.
- Netgear DC112A.

Con un puntaje de 6.1 en CVSS Meta Temp Score, esta vulnerabilidad de desbordamiento de búfer en la funcionalidad de Universal Plug and Play (UPnP); ocasiona que un atacante pueda ejecutar código sin autenticación.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-050	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	18-marzo-2022	**Vulnerabilidad presente en tres equipos de marca NETGEAR puede ocasionar inyección de código remoto**	V 1.1

IV. VECTOR DE ATAQUE: Red

Mediante la manipulación de un input desconocido se genera una vulnerabilidad de clase desbordamiento de búfer; así mismo, esta explotación no requiere ninguna forma de autenticación. De momento, según la información recopilada no se dispone de un exploit disponible.

El VulDB Vector asociado es: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:X/RL:X/RC:R

V. IMPACTO:

A continuación, se menciona el impacto y la mitigación para esta vulnerabilidad.

CVE	IMPACTO	MITIGACIÓN
CVE-2022-24655	Confidencialidad: Media Integridad: Media Disponibilidad: Media	• Parea el equipo EX6100v1, el fabricante siguiere actualizar la versión de firmware; para ello visite el sitio: https://www.netgear.com/support/ • En referencia a CAX80 se deberá actualizar al firmware 2.1.3.7. • En referencia a DC112A se deberá actualizar al firmware 1.0.0.64.

Tabla 1. CVE y productos afectados.
Fuente: Aviso de seguridad NETGEAR

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Actualizar el firmware en los dispositivos afectados conforme las especificaciones del fabricante.
- A los PST que emplean estos equipos, se sugiere tomar los correctivos necesarios y seguir las indicaciones brindadas por el fabricante a través de su Aviso de Seguridad: https://kb.netgear.com/000064615/Security-Advisory-for-Pre-Authentication-Command-Injection-on-EX6100v1-and-Pre-Authentication-Stack-Overflow-on-Multiple-Products-PSV-2021-0282-PSV-2021-0288

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-050	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	18-marzo-2022	**Vulnerabilidad presente en tres equipos de marca NETGEAR puede ocasionar inyección de código remoto**	V 1.1

VII. REFERENCIAS:

MITRE, C. (18 de 03 de 2022). *CVE MITRE*. Obtenido de CVE MITRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24655

Netgear. (s.f.). *Netgear*. Obtenido de Netgear: https://www.netgear.com/

Netgear, S. A. (02 de 03 de 2022). *Security Advisory Netgear*. Obtenido de Security Advisory Netgear: https://kb.netgear.com/000064615/Security-Advisory-for-Pre-Authentication-Command-Injection-on-EX6100v1-and-Pre-Authentication-Stack-Overflow-on-Multiple-Products-PSV-2021-0282-PSV-2021-0288

VulDB. (18 de 03 de 2022). *VulDB*. Obtenido de VulDB: https://vuldb.com/es/?id.195436

ZONE, R. (s.f.). *REDES ZONE*. Obtenido de REDES ZONE: https://www.redeszone.net/contenidos/netgear/