Código:	EC-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
Fecha:	13-dic-2021		
TLP	TLP:BLANCO		
Versión:	1.0	**DISPOSITIVOS MIKROTIK SIGUEN SIENDO VULNERABLES A ATAQUES DE BOTNETS**	

I. DATOS GENERALES:

Clase de alerta: Instrucción

Tipo de incidente: Denegación de Servicio

Nivel de riesgo: Medio

II. INTRODUCCIÓN

MikroTik es un fabricante de enrutadores y dispositivos ISP inalámbricos a nivel mundial, se ha receptado información indicando que más de 300.000 enrutadores MikroTik por falta de actualizaciones siguen siendo indefensos ante vulnerabilidades críticas de botnets de malware usado para criptominería y ataques de denegación de servicios - DDoS.

Figura 1.- *Dispositivos MikroTik víctimas de actores de amenazas.* **Fuente**: Eclypsium

III. VECTOR DE ATAQUE:

MALWARE, FIRMWARE/OS UPDATE/INFRAESTRUCTURA DE RED

Investigadores de Eclypsium escanearon Internet en busca de dispositivos MikroTik que aún son vulnerables a los siguientes cuatro CVEs (Eclypsium, 2021):

Código:	EC-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
Fecha:	13-dic-2021		
TLP	TLP:BLANCO		
Versión:	1.0	**DISPOSITIVOS MIKROTIK SIGUEN SIENDO VULNERABLES A ATAQUES DE BOTNETS**	

- **CVE-2019-3977**: Validación insuficiente del origen del paquete de actualización. CVSS v3 - 7.5
- **CVE-2019-3978**: Envenenamiento de caché remoto no autenticado. CVSS v3 - 7.5
- **CVE-2018-14847:** Escritura y acceso remoto a archivos arbitrarios no autenticados. CVSS v3 - 9.1
- **CVE-2018-7445:** Desbordamiento de búfer que permite el acceso remoto y la ejecución de código. CVSS v3 - 9.8

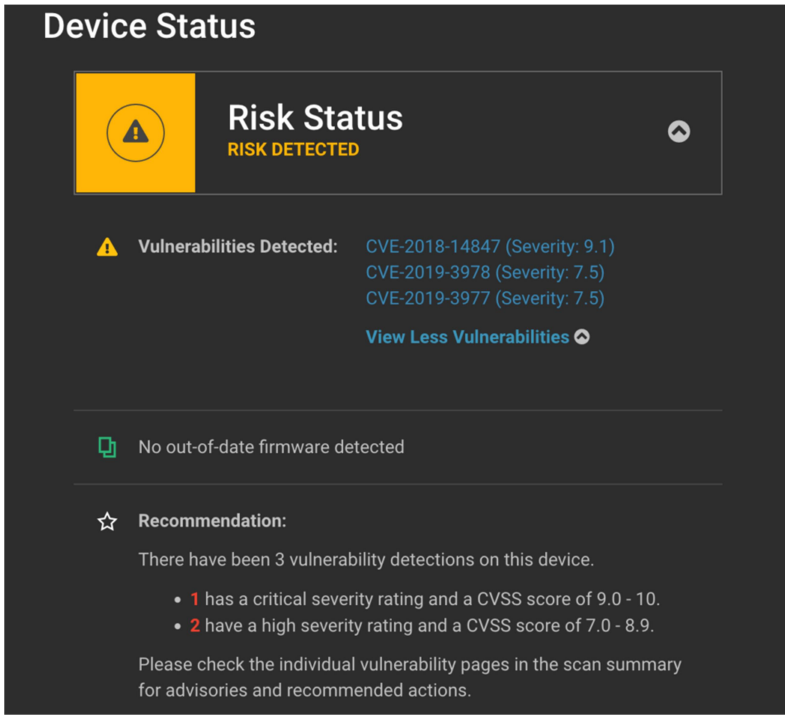

Figura 2.- Disponibilidad de herramientas para confirmar equipos mikrotik vulnerables **Fuente:** Eclypsium

Los CVEs listan aproximadamente 300.000 direcciones IP de hardware Mikrotik que detallan las siguientes características en los dispositivos:

Código:	EC-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
Fecha:	13-dic-2021		
TLP	TLP:BLANCO		
Versión:	1.0	**DISPOSITIVOS MIKROTIK SIGUEN SIENDO VULNERABLES A ATAQUES DE BOTNETS**	

- Dispositivos con protocolo WinBox expuestos
- Dispositivos con la versión RouterOS <= 6.45.6

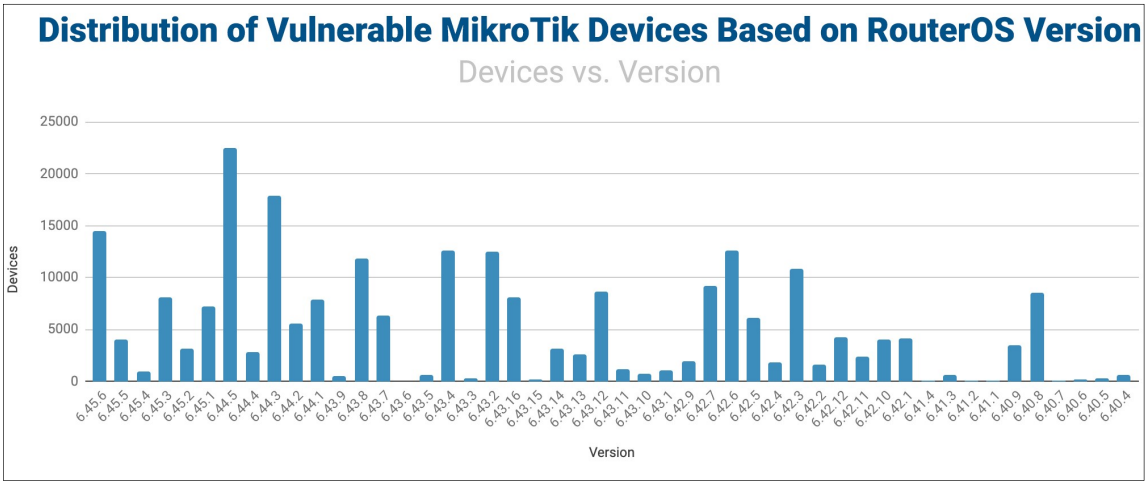

Figura 3.- Distribución de dispositivos Mikrotik vulnerables **Fuente:** Eclypsium

IV. IMPACTO:

Eclypsium encontró aproximadamente 300.000 direcciones IP para enrutadores MikroTik que cumplen con los criterios anteriores y son vulnerables al menos a una de las vulnerabilidades mencionadas anteriormente.

Estos dispositivos son generalmente utilizados por ISPs locales para redes SOHO (Small Office/Home Office) y IoT, a menudo vienen con credenciales predeterminadas de administrador / contraseña vacía, e incluso los dispositivos destinados a entornos corporativos vienen sin configuraciones predeterminadas para el puerto WAN. Además, la función de actualización automática de MikroTik rara vez se activa, lo que significa que muchos dispositivos simplemente nunca se actualizan. Todo esto conduce a utilizar dispositivos vulnerables y EOL fácilmente detectables en Internet, algunos de ellos con más de una década convirtiéndolos en objetivos atractivos para la criptominería y los ataques distribuidos de denegación de servicio.

Código:	EC-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
Fecha:	13-dic-2021		
TLP	TLP:BLANCO		
Versión:	1.0	**DISPOSITIVOS MIKROTIK SIGUEN SIENDO VULNERABLES A ATAQUES DE BOTNETS**	

Bleeping Computer se ha puesto en contacto con MikroTik para obtener un comentario sobre lo anterior y obtuvo la siguiente respuesta:

> *Eclypsium report deals with the same old vulnerabilities we have mentioned in our previous security blogs. As far as we know - there are no new vulnerabilities in RouterOS. Furthermore, RouterOS has been recently independently audited by several third parties. They all arrived at the same conclusion.*
>
> *Unfortunately, closing the old vulnerability does not immediately protect the affected routers. We don't have an illegal backdoor to change the user's password and check their firewall or configuration. These steps must be done by the users themselves.*
>
> *We try our best to reach out to all users of RouterOS and remind them to do software upgrades, use secure passwords, check their firewall to restrict remote access to unfamiliar parties, and look for unusual scripts. Unfortunately, many users have never been in contact with MikroTik and are not actively monitoring their devices. We cooperate with various institutions worldwide to look for other solutions as well.*
>
> *Meanwhile, we want to stress the importance of keeping your RouterOS installation up to date once again. That is the essential step to avoid all kinds of vulnerabilities.*

V. RECOMENDACIONES:

- Mantener actualizado los equipos periódicamente.
- Usar contraseñas seguras para el entorno de configuración y cambiarlas periódicamente.
- Verificar las configuraciones del equipo y solo habilite las funcionalidades que se requiera.
- Mantener el control de acceso al internet.

VI. REFERENCIAS:

Eclypsium. (09 de 12 de 2021). Obtenido de https://eclypsium.com/2021/12/09/when-honey-bees-become-murder-hornets/

Código:	EC-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
Fecha:	13-dic-2021		
TLP	TLP:BLANCO		
Versión:	1.0	**DISPOSITIVOS MIKROTIK SIGUEN SIENDO VULNERABLES A ATAQUES DE BOTNETS**	

Toulas, B. (09 de 12 de 2021). *Bleepingcomputer*. Obtenido de https://www.bleepingcomputer.com/news/security/hundreds-of-thousands-of-mikrotik-devices-still-vulnerable-to-botnets/