



Nro. Alerta:	EC-2022-029	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	 TLP:BLANCO		
Fecha:	14-febrero-2022	Vulnerabilidades de seguridad utilizadas activamente en ataques cibernéticos	V 1.0

I. DATOS GENERALES:

Clase de alerta:	Sistema(s) Vulnerable(s)
Tipo de incidente:	Vulnerabilidad
Nivel de riesgo:	Alto

II. ALERTA

Sistemas de Microsoft, Apache, D-LINK, Apple, Oracle, entre otros, podrían verse amenazados y ser víctimas de comprometimiento de datos y acceso no autorizado a cuentas confidenciales, debido a vulnerabilidades de seguridad que se utilizan activamente en ataques cibernéticos.





Figura 1. Common Vulnerabilities and Exposures Fuente: CVE ORG

III. INTRODUCCIÓN

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha agregado al catálogo de vulnerabilidades otros 15 problemas de seguridad que se utilizan activamente en los ataques cibernéticos. Los administradores de sistemas deben priorizar la instalación de actualizaciones de seguridad para proteger la infraestructura de red de sus organizaciones.

Son 15 las vulnerabilidades (CVEs) listadas, las cuales van desde 2014 hasta 2021, y se detallan en la Tabla Nro. 1 a continuación:





Nro. Alerta:	EC-2022-029	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	 <p>CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT</p>
TLP:	 TLP:BLANCO		
Fecha:	14-febrero-2022	Vulnerabilidades de seguridad utilizadas activamente en ataques cibernéticos	V 1.0

ID de CVE	Descripción	Fecha límite del parche
CVE-2021-36934	Vulnerabilidad de escalada de privilegios locales SAM de Microsoft Windows	2/24/2022
CVE-2020-0796	Vulnerabilidad de ejecución remota de código de Microsoft SMBv3	8/10/2022
CVE-2018-1000861	Jenkins Stapler Web Framework Deserialización de datos no confiables	8/10/2022
CVE-2017-9791	Vulnerabilidad de validación de entrada incorrecta de Apache Struts 1	8/10/2022
CVE-2017-8464	Ejecución remota de código de Microsoft Windows Shell (.lnk)	8/10/2022
CVE-2017-10271	Oracle Corporation WebLogic Server Ejecución remota de código	8/10/2022
CVE-2017-0263	Vulnerabilidad de escalada de privilegios de Microsoft Win32k	8/10/2022
CVE-2017-0262	Vulnerabilidad de ejecución remota de código de Microsoft Office	8/10/2022
CVE-2017-0145	Vulnerabilidad de ejecución remota de código de Microsoft SMBv1	8/10/2022
CVE-2017-0144	Vulnerabilidad de ejecución remota de código de Microsoft SMBv1	8/10/2022
CVE-2016-3088	Vulnerabilidad de validación de entrada incorrecta de Apache ActiveMQ	8/10/2022
CVE-2015-2051	Ejecución remota de código del enrutador D-Link DIR-645	8/10/2022
CVE-2015-1635	Vulnerabilidad de ejecución remota de código de Microsoft HTTP.sys	8/10/2022
CVE-2015-1130	Vulnerabilidad de omisión de autenticación de Apple OS X	8/10/2022
CVE-2014-4404	Vulnerabilidad de desbordamiento de búfer basado en almacenamiento dinámico de Apple OS X	8/10/2022

Tabla 1. Principales CVEs utilizadas activamente en ciberataques Fuente: BleepingComputer



Nro. Alerta:	EC-2022-029	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	 <p>CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT</p>
TLP:	 TLP:BLANCO		
Fecha:	14-febrero-2022	Vulnerabilidades de seguridad utilizadas activamente en ataques cibernéticos	V 1.0

IV. VECTOR DE ATAQUE

Local, Red

V. IMPACTO

De la Tabla Nro. 1, destaca la CVE-2021-36934. Esta es una vulnerabilidad SAM (Administrador de cuentas de seguridad) de Microsoft Windows que permite a cualquier persona acceder a los archivos de la base de datos del Registro en Windows 10 y 11, extraer hashes de contraseñas y obtener privilegios de administrador.

Microsoft solucionó esta falla en julio de 2021, pero siete meses después todavía hay una cantidad importante de sistemas que necesitan instalar la actualización.

La CVE-2020-0796 es otra falla de seguridad crítica que los administradores deben abordar. El error recibió la máxima puntuación de gravedad. Consiste en el manejo erróneo de paquetes de datos comprimidos malintencionados por parte de SMBv3 (Server Message Block protocol) y puede ser explotado para lograr la ejecución remota de código. En marzo de 2020, había al menos 48 000 sistemas vulnerables a ésta vulnerabilidad, y, el problema persiste.

Vulnerabilidad CVE-2015-2051, un error de ejecución remoto de código, el cual afecta a los enrutadores D-Link DIR-645 y, continúa expuesto a ciberataques.



Los informes más recientes de explotación de la vulnerabilidad particular, datan de noviembre de 2021, cuando la red de bots BotenaGo apuntó a millones de dispositivos y enrutadores IoT a través de un conjunto de 33 vulnerabilidades conocidas, incluida CVE-2015-2051.

VI. RECOMENDACIONES

El EcuCERT, recomienda a su comunidad objetivo, tomar en consideración lo siguiente:

- Mantener siempre al día las actualizaciones de todos los sistemas de hardware/software existentes, tanto a nivel de sistema operativo como de firmware.
- Instituciones/Organizaciones deben ocuparse de la actualización o repotenciación del hardware obsoleto e incompatible presente en lugares sensibles de su infraestructura de red.
- Utilizar software antivirus de confianza, en computadores y dispositivos móviles.



Nro. Alerta:	EC-2022-029	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	 <p>CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT</p>
TLP:	 TLP:BLANCO		
Fecha:	14-febrero-2022	Vulnerabilidades de seguridad utilizadas activamente en ataques cibernéticos	V 1.0

- Implementar un plan de respuesta a emergencias en la Organización/Institución, considerar la gama completa de impactos potenciales que los ciberataques plantean a las operaciones, incluida la pérdida o manipulación de la información, la pérdida o manipulación del control y, las amenazas a la seguridad.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

VII. REFERENCIAS:

Bill Toulas. (11 de febrero de 2022). BleepingComputer. Obtenido de <https://www.bleepingcomputer.com/news/security/cisa-urges-orgs-to-patch-actively-exploited-windows-serioussam-bug/>

CISA. (10 de febrero de 2022). CISA. Obtenido de <https://www.cisa.gov/uscert/ncas/current-activity/2022/02/10/cisa-adds-15-known-exploited-vulnerabilities-catalog>

