Nro. Alerta:	EC-2021-038	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES EcuCERT **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	30-dic-2021	ILOBleed: Malware tipo RootKit dirigido a servidores de la marca Hewlett-Packard tipo Integrated Lights-Out iLO	V 1.0

I. DATOS GENERALES:

Clase de alerta: Malware

Tipo de incidente: RootKit / escalamiento de privilegios

Nivel de riesgo: Medio

II. ALERTA

Nuevo rootkit, previamente desconocido, se enfoca en tecnología de administración de servidor Integrated Lights-Out (iLO) de Hewlett-Packard Enterprise para llevar a cabo ataques que manipulan los módulos de firmware y borran por completo los datos de los sistemas infectados.

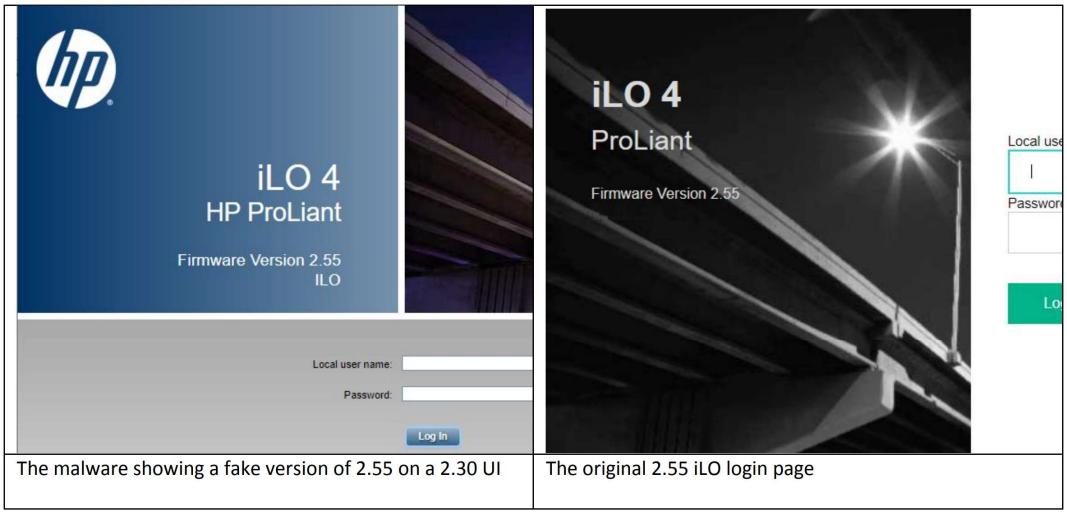
III. INTRODUCCIÓN

Servidores de la marca Hewlett-Packard, proporcionan un módulo de gestión llamado iLO (también conocido como Integrated Lights-Out); éste módulo, se enciende tan pronto como se conecta el cable de alimentación, cargando un sistema operativo patentado, el cual tiene acceso completo a todo el firmware, hardware, software y sistema operativo instalados en el servidor. Además de administrar el hardware del servidor, permite al administrador encender y apagar el servidor de forma remota, obtener acceso a la consola del servidor e incluso instalar un sistema operativo en él.

Investigadores de Amnpardaz Soft, analizaron un rootkit que se esconde dentro de iLO, el cual no se puede eliminar mediante actualizaciones de firmware y se puede ocultar a la vista durante mucho tiempo. Este malware ha sido utilizado por piratas informáticos durante algún tiempo y su rendimiento ha sido monitoreado.

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-2021-038	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES EcuCERT **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	30-dic-2021	ILOBleed: Malware tipo RootKit dirigido a servidores de la marca Hewlett-Packard tipo Integrated Lights-Out iLO	V 1.0



The malware showing a fake version of 2.55 on a 2.30 UI | The original 2.55 iLO login page

Figura No. 1: Comparación entre Interfaz infectada vs real de portal de ingreso a sistema HP iLO
Fuente: Amnpardaz Soft

IV. VECTOR DE ATAQUE

Puede ser a través de Red y Local.

V. IMPACTO

El panel de administración de iLO de los servidores HP es un sitio seguro para el malware que, después de la infección, no puede detectarse ni limpiarse con métodos convencionales.

Acceder e infectar iLO no solo es posible a través del puerto de red de iLO, sino también a través del administrador del sistema o del acceso root al sistema operativo principal. Esto significa que, si un intruso tiene acceso a un usuario con privilegios de administrador / root en el sistema operativo principal instalado en el servidor, puede, sin necesidad de autenticación adicional, comunicarse directamente con iLO e infectarlo si es vulnerable.

La investigación a lo largo de los años ha revelado varias vulnerabilidades en HP iLO que han dado lugar a parches y cambios de arquitectura por parte del fabricante.

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-2021-038	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES EcuCERT **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	30-dic-2021	ILOBleed: Malware tipo RootKit dirigido a servidores de la marca Hewlett-Packard tipo Integrated Lights-Out iLO	V 1.0

En iLO4 y sus versiones anteriores utilizadas en servidores G9 e inferiores, no existe un mecanismo de arranque seguro con una clave raíz de confianza incorporada en el hardware. Por lo tanto, el firmware de estas versiones tiene más riesgo de ser modificado e infectado por malware.

Incluso si iLO se ha actualizado a la última versión que no tiene vulnerabilidades conocidas, aún es posible degradarlo a una versión inferior, lo que hace posible infectar el firmware completamente parcheado. Solo puede evitar esto en la serie G10 si está habilitada una configuración no predeterminada. En servidores anteriores, no es posible evitar el mecanismo de degradación.

Dado lo anterior, las soluciones simples como desconectar por completo el cable de red de iLO o actualizar el firmware a la última versión NO son suficientes para prevenir una infección de malware.

Desde 2020, el equipo de análisis de malware de Amnpardaz Software Company ha descubierto un rootkit que agrega un módulo malicioso llamado Implant.ARM.iLOBleed.a al firmware de iLO y modifica varios módulos de firmware originales. El rootkit evita silenciosamente las actualizaciones de firmware mientras finge que se completa. También proporciona acceso al hardware del servidor; uno de cuyos resultados es una limpieza completa de los discos del servidor.

VI. INDICADORES DE COMPROMISO

Es habitual proporcionar hash como IOC, sin embargo esto no será efectivo contra este malware. Principalmente porque sin tener una herramienta de volcado de iLO a mano, será imposible leer el firmware y verificar su hash. Además, el conjunto de firmware de iLO real es muy pequeño, por lo que adoptar un enfoque de lista blanca es posible y más adecuado. (es decir, comparar el hash del firmware con una lista de buenos hash conocidos).

Sin embargo, el malware se esfuerza por simular el proceso de actualización y tiene dificultades para mostrar versiones falsas "actualizadas" en la interfaz de usuario web de iLO y en otros lugares, sin embargo, HP cambió considerablemente la interfaz de usuario de iLO. Por lo tanto, puede detectar fácilmente la presencia de malware a simple vista después de hacer una copia del firmware del servidor **(Figura No. 1)**, debe compararse con las versiones originales del firmware.

El malware Implant.ARM.iLOBleed.a se basa en la versión 2.30 del firmware de iLO. En consecuencia, la diferencia entre esta versión infectada y la versión original se muestra en la siguiente figura **(Figura No. 2)**.

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-2021-038	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES EcuCERT **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	30-dic-2021	ILOBleed: Malware tipo RootKit dirigido a servidores de la marca Hewlett-Packard tipo Integrated Lights-Out iLO	V 1.0

Figura No. 2: Diferencia de firmas de firmware: (Arriba) Volcado infectado obtenido; (Abajo) Versión original proporcionada por HP Company
Fuente: Amnpardaz Soft

Diferencia (Bytes)	MD5 (infectado)	MD5 (original)	Nombre del módulo
15,625 MB	4f8417af3a6f75780e09c5792397a05f	98af47cb8cacb25abd333d8a1a752c6b	hpimage.bin
0	8433650ef98fd8790877e6616c02b66c	8433650ef98fd8790877e6616c02b66c	hpimage.hdr
0	ae22d82a3e954ecf911b834463dbfbbe	ae22d82a3e954ecf911b834463dbfbbe	bootloader.hdr
5 B	1fdb4270665177ecb1c9708039bab934	20ff78c6604563c27b6f9c75775c9306	bootloader.bin
2 B	7df3b258ca3c12f0f8de77469456e25d	e1b1244fead44f73efb7b559e9d719c9	kernel_main.hdr
12 B	9ab97c5b03664da18ab1f775dc11c200	bacc259ea63785607faf2dab6939a2db	kernel_main.bin
2 B	7df3b258ca3c12f0f8de77469456e25d	e1b1244fead44f73efb7b559e9d719c9	kernel_recovery.hdr
12 B	9ab97c5b03664da18ab1f775dc11c200	bacc259ea63785607faf2dab6939a2db	kernel_recovery.bin
2 B	64d0143d638885745b241796268eb0b2	7db6ebd698fa4862cfde68a546e9a75b	ELF.hdr
15,625 MB	bdeeab3994ec5d0b93d961148a6b712d	d16fee481f78ad0275dd29ed271582aa	ELF.bin

Tabla No. 1: Compare las firmas de los módulos de firmware del sistema infectado con la versión original
Fuente: Amnpardaz Soft

Nro. Alerta:	EC-2021-038	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES EcuCERT **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	30-dic-2021	ILOBleed: Malware tipo RootKit dirigido a servidores de la marca Hewlett-Packard tipo Integrated Lights-Out iLO	V 1.0

VII. RECOMENDACIONES

El Centro de Respuestas a Incidentes Informáticos de la ARCOTEL, 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.
- No conectar la interfaz de red de Hewlett-Packard iLO a la red operativa.
- Realizar la configuración de seguridad de iLO en los servidores Hewlett-Packard y desactivar la degradación para los servidores G10.
- Utilizar estrategias de defensa en profundidad para reducir el riesgo y detectar intrusiones antes de llegar a sistemas tipo Hewlett-Packard iLO.
- Utilizar periódicamente la herramienta Hewlett-Packard iLO Scanner para detectar posibles vulnerabilidades, malware y puertas traseras en la versión actual del firmware del servidor iLO.
- Estar pendiente a la herramienta que próximamente se lanzará al público una para verificar la integridad del firmware HP iLO.
- Realizar copias de respaldo de seguridad periódicas, de toda la información, datos y de configuraciones, para evitar la pérdida de información.
- 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.

VIII. REFERENCIAS:

- Ravie Lakshmanan. (30 de diciembre de 21). TheHackerNews. Obtenido de https://thehackernews.com/2021/12/new-ilobleed-rootkit-targeting-hp.html
- Amnpardaz Soft. (30 de diciembre de 2021). Amnpardaz Soft. Obtenido de https://threats.amnpardaz.com/en/2021/12/28/implant-arm-ilobleed-a/

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