Open-IPMI (Intelligent Platform Management Interface)

1. INTRODUCCIÓN

IPMI es una especificación de interfaz de bajo nivel adoptado por algunos fabricantes de hardware, que permite a un administrador gestionar de forma remota servidores a nivel de hardware. IPMI se ejecuta en el controlador de administración de placa base (BMC=Baseboard Management Controller) y proporciona acceso a la BIOS, discos y otro tipo de hardware. La BMC tiene un conjunto limitado de servicios de red para facilitar la gestión y la comunicación entre los sistemas.

IPMI permite gestionar servidores con independencia del sistema operativo; y además, permite la administración de los sistemas a través de la red. Al funcionar con independencia del sistema operativo, los administradores pueden acceder a los sistemas y reestablecerlos aún en el caso de que el sistema operativo no responda.

2. RIESGO

Cualquier sistema conectado al internet a través de la Interfaz IPMI puede verse afectado. Los atacantes pueden utilizar IPMI para obtener acceso a nivel físico del servidor, reiniciar el sistema, instalar un nuevo sistema operativo, comprometer datos, sin necesidad de pasar por ningún control del sistema operativo.

Un atacante con conocimiento de IPMI puede identificar fácilmente sistemas con acceso a esta interfaz IPMI que están conectados a la Internet. Muchas de estas interfaces utilizan claves por defecto, sin contraseñas o cifrado débil. Con lo cual el atacante puede comprometer la confidencialidad, integridad y disponibilidad del servidor al acceder a la BMC.

PRODUCTOS AFECTADOS

Servidores HP Integrated Lights Out, Dell DRAC y adaptadores de supervisión remota de IBM.

3. DETECCIÓN

Agencia de Regulación y Control de las Telecomunicaciones	**SEGURIDAD DE LA INFORMACIÓN**	ecucert Centro de Respuesta a Incidentes Informáticos
	VULNERABILIDAD OPEN IPMI	

El reporte de “Open IPMI SCANNING” se basa en peticiones IPMI al puerto 623/udp de hosts con direcciones IPv4, con el fin de identificar dispositivos accesibles y reportarlos a los propietarios de la red.

La comprobación se realiza usando el siguiente comando en Linux:

ipmitool -A NONE -H [IP] bmc info

INFORMACIÓN DE LOS CAMPOS DEL REPORTE:

Campo	Descripción
Vulnerabilidad	Nombre de la vulnerabilidad reportada
Dirección IP	Dirección IP del host
Puerto	Puerto desde donde se obtiene la respuesta
timestamp_EcuCERT	Fecha y hora de comprobación de EcuCERT en GMT -5
status_EcuCERT	Online: vulnerabilidad reportada por Feeds y comprobada por el EcuCERT en el timestamp_EcuCERT Offline: Vulnerabilidad reportada por Feeds, pero en el timestamp_EcuCERT no se detectó.
as_name	Nombre del ASN al que pertenece la dirección IP
timestamp	Fecha y hora de comprobación en UTC+0
ip	Dirección IP del host
protocol	Protocolo por el que la respuesta IPMI ingresa (UDP)
port	Puerto desde donde se obtiene la respuesta IPMI
hostname	DNS reverso del host
asn	ASN donde se encuentra el host
geo	País donde se encuentra el host
region	Estado / Provincia / Región donde se encuentra el host
city	Ciudad donde se encuentra el host
ipmi_version	Version de IPMI (version 1.5 or 2.0)
none_auth	Ningún Soporte de mecanismo de autenticación (yes = malo)
md2_auth	Soporte a autenticación MD2 (yes = malo)
md5_auth	Soporte a autenticación MD5
passkey_auth	Soporta clave de autenticación (yes = malo)
oem_auth	Soporta mecanismos propietarios de autenticación (se desconoce si es bueno o malo)
defaultkg	Solo IPMI v2.0. Estado de autenticación de inicio de sesión de dos claves. (default significa que la clave se establece en todo cero)
permessage_auth	Estado de autenticación Per-message (disabled es malo)
userlevel_auth	Estado de autenticación de nivel de usuario (disabled es malo)
usernames	Usuarios Non-Null están habilitado (al menos una cuenta está habilitada con non-null)
nulluser	Usuario NULL están habilitados con contraseñas no NULL

Campo	Descripción
anon_login	Inicios de sesión anónimos están permitidos (usuario NULL y una contraseña NULL) (sí = malo)
error	(IPMI v1.5 "none" authentication only) Condición de error. reportado cuando una prueba "info" se envía a la BMC
deviceid	(IPMI v1.5 "none" authentication only) ID del dispositivo: Especificado por el fabricante
devicerev	(IPMI v1.5 "none" authentication only) Revisión del dispositivo: Número de revisión de la prueba BMC
firmwarerev	(IPMI v1.5 "none" authentication only) Version de Firmware:
version	(IPMI v1.5 "none" authentication only) version IPMI:
manufacturerid	(IPMI v1.5 "none" authentication only) ID del fabricante: Nombre del fabricante en formato SMI Network Management Private Enterprise Code
manufacturername	(IPMI v1.5 "none" authentication only) Nombre del Fabricante
productid	(IPMI v1.5 "none" authentication only) ID del producto
productname	(IPMI v1.5 "none" authentication only) Nombre del producto

4. ACCIONES RECOMENDADAS

- Restringir el acceso a la interfaz IPMI a direcciones IP de la red interna de administración.
- Restringir el tráfico IPMI a una VLAN.
- Deshabilitar IPMI si no se necesita
- Utilizar contraseñas seguras, limitar el número de intentos fallidos
- Habilitar la encripción de tráfico de ser posible (consultar manual del fabricante).
- Requerir autenticación.
- Desactivar "cifrado 0" que es vulnerable, y los inicios de sesión anónimos. "cipher 0" es una opción habilitada por defecto en muchos dispositivos habilitados para IPMI.
- Usar ACLs
- Al fin de la vida útil del equipo, Eliminar la información de la memoria Flash donde la contraseña IPMI pueda almacenarse.

5. REFERENCIAS

- https://ipmiscan.shadowserver.org/
- https://www.shadowserver.org/wiki/pmwiki.php/Services/Open-IPMI

https://www.us-cert.gov/ncas/alerts/TA13-207A