PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

130-2025-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aéreadel Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y lasempresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°130	Fecha: 05-06-2025
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Actualización de los Indicadores de Compromiso del Ransomware PLAY		
Tipo de Ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Desde junio de 2022, el grupo de ransomware Play (también conocido como Playcrypt) ha afectado a una amplia gama de empresas e infraestructuras críticas en Norteamérica, Sudamérica y Europa. Play fue uno de los grupos de ransomware más activos en 2024.

La Oficina Federal de Investigaciones (FBI), la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) y el Centro Australiano de Seguridad Cibernética de la Dirección de Señales de Australia (ACSC, por sus siglas en inglés) están publicando este aviso conjunto para difundir los IOC y TTP del grupo de ransomware Play identificados a través de investigaciones del FBI en enero de 2025

2. DETALLES:

El grupo de ransomware Play obtiene acceso inicial a las redes de sus víctimas mediante el uso indebido de cuentas válidas, probablemente adquiridas en la dark web, y la explotación de aplicaciones públicas, principalmente a través de vulnerabilidades conocidas de FortiOS (CVE-2018-13379 y CVE-2020-12812) y Microsoft Exchange (CVE-2022-41040 y CVE-2022-41082).

También se ha observado que los actores del ransomware Play utilizan servicios externos como el Protocolo de Escritorio Remoto (RDP) y las Redes Privadas Virtuales (VPN) para el acceso inicial.

El grupo de ransomware Play utiliza un modelo de doble extorsión [T1657], cifrando los sistemas tras exfiltrar datos. La nota de rescate indica a las víctimas que se pongan en contacto con el grupo de ransomware Play a una dirección de correo electrónico terminada en [nombre del grupo]@gmx[.]de o [nombre del grupo]@web[.]de.

Los pagos del rescate se realizan en criptomonedas a las direcciones de billetera proporcionadas por los actores de Play. Si una víctima se niega a pagar el rescate, los actores del ransomware amenazan con publicar los datos exfiltrados en su sitio de filtración en la red Tor [.]onionURL.

Las víctimas del ransomware Play reciben regularmente llamadas telefónicas de actores de amenazas que les instan a pagar y amenazan con divulgar información de la empresa. Estas llamadas pueden dirigirse a diversos números de teléfono dentro de la organización, incluidos aquellos descubiertos en código abierto, como centros de ayuda o representantes de atención al cliente.

La variante ESXi del ransomware Play invoca comandos de shell específicos del entorno ESXi para realizar tareas, como apagar todas las máquinas virtuales (VM) en ejecución, listar los nombres de las máquinas y configurar el mensaje de bienvenida de la interfaz ESXi para la nota de rescate específica de la campaña.

El binario del ransomware admite argumentos de línea de comandos; sin embargo, si no se pasan, el malware apaga todas las VM y cifra los archivos relacionados con ellas mediante claves generadas aleatoriamente por archivo. Las extensiones del archivo objetivo incluyen .vmdk, .vmem, .vmsd, .vmsn, .vmx, .vmxf, .vswp, .vmss, .nvram, .vmtx, y .log. El binario del ransomware utiliza AES-256 como algoritmo de cifrado. Crea una copia de la nota de rescate titulada PLAY_Readme.txten el directorio raíz y en la ruta /vmfs/volumes/, así como el mensaje de bienvenida de la interfaz ESXi.

Los atacantes del ransomware Play utilizan herramientas como AdFind para ejecutar consultas de Active Directory [TA0007] y Grixba, un ladrón de información, para enumerar información de red [T1016] y buscar software antivirus. También utilizan herramientas como GMER, IOBit y PowerTool para desactivar el software antivirus y eliminar archivos de registro. También han utilizado scripts de PowerShell para atacar Microsoft Defender.

Los actores del ransomware Play utilizan aplicaciones de comando y control (C2), como Cobalt Strike y SystemBC, y herramientas como PsExec para facilitar el movimiento lateral y la ejecución de archivos. Una vez establecidos en una red, buscan credenciales no seguras [T1552] y utilizan el volcador de credenciales Mimikatz para obtener acceso de administrador de dominio [T1003].

Indicadores de Compromiso:

Hashes (SHA 256 y SHA 1)	**Descripción**
47B7B2DD88959CD7224A5542AE8D5BCE928BFC986BF0D0321532A7515C244A1E	SVCHost.dll Puerta trasera
75B525B220169F07AECFB3B1991702FBD9A1E170CAF0040D1FCB07C3E819F54A 453257C3494ADDAFB39CB6815862403E827947A1E7737EB8168CD10522465DEB C59F3C8D61D940B56436C14BC148C1FE98862921B8F7BAD97FBC96B31D71193C	GRIXBA Gt_net.exe Herramienta de recopilación de datos personalizada
1409E010675BF4A40DB0A845B60DB3AAE5B302834E80ADEEC884AEBC55ECCBF7	PSexesvc.exe Juego personalizado “psexesvc”
0E408AED1ACF902A9F97ABF71CF0DD354024109C5D52A79054C421BE35D93549	HRsword.exe Desactiva la protección de puntos finales
90040340EE101CAC7831D7035230AC8AD4224D432E5636F34F13AA1C4A0C2041	Usysdiag.exe Asociado con HRsword; cambia la configuración de los certificados del sistema
3D86555ACAA19AEDDB5896071D1E3711B062EDBE	fThe9C.exe
6DE8DD5757F9A3AC5E2AC28E8A77682D7A29BE25C106F785A061DCF582A20DC6	Hi.exe Asociado con ransomware
75404543DE25513B376F097CEB383E8EFB9C9B95DA8945FD4AA37C7B2F226212	Malware EXE de SystemBC
7A42F96599DF8090CF89D6E3CE4316D24C6C00E499C8557A2E09D61C00C11986 7DEA671BE77A2CA5772B86CF8831B02BFF0567BCE6A3AE023825AA40354F8ACA	DLL de malware de SystemBC
967DAFF362E63FF45526F585B7944488ACE1BB5BB5B30FA40D56557F1C538D09	SHA256 Hash de la clave pública ECDSA
859165041D75FBA3759C5533E324225F355C8A07B4645B984192AD6BEF06DB1A	SHA-256 Hash de la clave pública ED25519 para el servidor WinSCP
511F63455CA4F83B0347B65DDA17585AD02591A9F23D8E234E5CE1321AA3381A	SHA-256 Hash de la clave pública ED25519 del servidor WinSCP
372F7B45A141BB0709D578BC716CBCA03104258822C4290CCBEB600223850158	SHA-256 Hash de la clave pública ED25519 del servidor WinSCP

3. RECOMENDACIONES:

- Realizar el bloqueo de cualquier indicador de compromiso identificado asociado a algún ransomware.
- Deshabilitar los puertos de acceso remoto/Protocolo de escritorio remoto (RDP) no utilizados y monitorear los registros de acceso/RDP.
- Ejecutar la estrategia 3-2-1-1-0 de copias de seguridad, que consiste en realizar periódicamente tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube; además una de las copias esté disponible fuera de conexión, y cero copias sin verificar o con errores.
- Implementar un plan de recuperación para mantener y conservar múltiples copias de datos y servidores confidenciales o propietarios en una ubicación físicamente separada, segmentada y segura.
- Desarrollar planes de respuesta ante incidentes que abarquen toda la cadena de suministro.
- Cifrar las copias realizadas. Así, incluso si se ven comprometidas, serían indescifrables e inútiles para el atacante.
- Priorizar la reparación de vulnerabilidades explotadas conocidas, especialmente para correo web, VPN y cuentas que acceden a sistemas críticos.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Habilitar la autenticación multifactor (MFA) para todos los servicios en la medida de lo posible.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial de las infecciones de ransomware y auditar cuentas de usuario con privilegios administrativos
- Segmentar redes para restringir el movimiento lateral desde los dispositivos infectados.
- Invertir en soluciones de seguridad, como sistemas de detección y respuesta de endpoints (EDR), y software de detección y prevención de intrusiones (IDS/IPS), que utilicen inteligencia artificial y aprendizaje automático para la detección proactiva de amenazas, de tal manera que pueda identificar y bloquear comportamientos sospechosos antes de que causen daños significativos.
- Habilitar la protección de red para evitar que las aplicaciones o los usuarios accedan a dominios maliciosos y otro contenido malicioso en Internet.
- Revisar los controladores de dominio, servidores, estaciones de trabajo y directorios activos en busca de cuentas nuevas o no reconocidas.
- Procurar que todas las cuentas con inicios de sesión con contraseña (por ejemplo, cuentas de servicio, cuentas de administrador y cuentas de administrador de dominio) cumplan con los estándares del NIST para el desarrollo y la gestión de políticas de contraseñas, incluyendo longitud mínima, complejidad, no reutilización, bloqueo ante intentos fallidos, caducidad, etc.
- Habilitar la protección de firewall para monitorear y controlar el tráfico de red entrante y saliente.
- Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet (fuga de informaciones). Es importante prestar especial atención al tráfico saliente para detectar las conexiones de los ciberdelincuentes en su red.
- Promover la cooperación global en el intercambio de información sobre amenazas, el desarrollo de marcos regulatorios y el fortalecimiento de capacidades de respuesta ante incidentes.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a • hxxps://www.cisa.gov/stopransomware/ransomware-tips

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°130	Fecha: 05-06-2025 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en múltiples productos Cisco		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Cisco Systems, Inc. ha publicado una vulnerabilidad de severidad **ALTA** de tipo restricción inadecuada del canal de comunicación a los puntos finales previstos que afecta a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado acceder a servicios internos con privilegios elevados.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-20261 de tipo restricción inadecuada del canal de comunicación a los puntos finales previstos en el manejo de la conexión SSH de Cisco Integrated Management Controller (IMC) para servidores Cisco UCS B-Series, UCS C-Series, UCS S-Series y UCS X-Series, podría permitir que un atacante remoto autenticado acceda a servicios internos con privilegios elevados.

Esta vulnerabilidad se debe a restricciones insuficientes de acceso a los servicios internos. Un atacante con una cuenta de usuario válida podría explotar esta vulnerabilidad utilizando una sintaxis manipulada al conectarse a Cisco IMC de un dispositivo afectado mediante SSH. Una explotación exitosa podría permitir al atacante acceder a servicios internos con privilegios elevados, lo que podría permitir modificaciones no autorizadas en el sistema, incluyendo la posibilidad de crear nuevas cuentas de administrador en el dispositivo afectado.

A. Productos afectados:

Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión de software vulnerable y aceptan conexiones SSH entrantes a Cisco IMC:

- UCS B-Series Blade Servers.
- UCS C-Series Rack Servers.
- UCS S-Series Storage Servers.
- UCS X-Series Modular System.

3. RECOMENDACIONES:

- Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas.
- Considerar las siguientes propiedades para efectos de mitigación:
  - Los servidores Cisco UCS serie C y UCS serie S en modo independiente aceptan conexiones SSH entrantes de forma predeterminada.
  - Los servidores Cisco UCS serie B, Managed UCS serie C, Managed UCS serie S y UCS serie X sólo aceptan conexiones SSH entrantes si la política de serie a través de LAN (SoL) está habilitada en el perfil de servicio asociado.
  - Los dispositivos Cisco basados en una versión preconfigurada de un servidor Cisco UCS C-Series también se ven afectados por esta vulnerabilidad si exponen el acceso SSH a Cisco IMC.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-ssh-priv-esc-2mZDtdjM

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°130	Fecha: 05-06-2025 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el router D-Link DIR-816		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo restricción incorrecta de operaciones dentro de los límites de un búfer de memoria en la versión 1.10CNB05 del firmware del router D-Link DIR-816. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la ejecución remota de código.

2. DETALLES:

D-Link DIR-816 es un enrutador inalámbrico AC750 de doble banda diseñado para uso doméstico y en pequeñas oficinas, que proporciona conectividad Wi-Fi confiable y de alta velocidad con una variedad de funciones avanzadas.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-5623 de tipo restricción incorrecta de operaciones dentro de los límites de un búfer de memoria en la versión 1.10CNB05 del firmware D-Link DIR-816 implica un desbordamiento de búfer basado en la pila en la función qosClassifier. Esta vulnerabilidad puede explotarse manipulando los argumentos dip_address o sip_address, lo que podría permitir a un atacante remoto no autenticado la ejecución remota de código.

Un ataque exitoso podría permitir a un atacante remoto obtener acceso no autorizado a la infraestructura de red, el robo de datos o infiltración en la red y comprometer el sistema debido a los altos impactos en la confidencialidad, integridad y disponibilidad.

Cabe señalar que el exploit para esta vulnerabilidad se ha hecho público y puede utilizarse. Esta vulnerabilidad solo afecta a los productos que ya no reciben soporte del mantenedor.

A. Productos afectados:

- D-Link DIR-816, versión de firmware 1.10CNB05.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Aislar inmediatamente los dispositivos afectados de las redes.
- Reemplazar los dispositivos D-Link DIR-816 no compatibles.
- Implementar la segmentación de la red para limitar el impacto potencial de la explotación.
- Utilizar sistemas de detección/prevención de intrusiones para monitorear posibles intentos de explotación.
- Deshabilitar la función qosClassifier vulnerable.

Fuente de Información:	• hxxps://github.com/wudipjq/my_vuln/blob/main/D-Link5/vuln_51/51.md • hxxps://github.com/wudipjq/my_vuln/blob/main/D-Link5/vuln_51/51.md • hxxps://vuldb.com/?ctiid.311109 • hxxps://vuldb.com/?id.311109 • hxxps://vuldb.com/?submit.589224

Índice alfabético