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

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 19 de enero de 2023

017-2023-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 Aérea del 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 las empresas 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° 017**	**Fecha: 19-01-2023**
		Página 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Detectan vulnerabilidades críticas de seguridad en routers de Netcomm y TP-Link		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

Cuatro vulnerabilidades críticas afectan a una serie de modelos concretos de routers de Netcomm y TP-Link pudiendo ejecutar código de forma remota y divulgar información.

DETALLES:

Las vulnerabilidades, registradas como CVE-2022-4873 y CVE-2022-4874, se refieren a un caso de desbordamiento de búfer y afectan a los modelos de router de Netcomm NF20MESH, NF20 y NL1902 que ejecutan versiones de software anteriores a R6B035.

Según el Centro de Coordinación CERT de la agencia de Ciberseguridad e Infraestructura del Departamento de Seguridad Nacional estadounidense, «las dos vulnerabilidades, cuando se encadenan juntas, permiten que un atacante remoto no autenticado ejecute código arbitrario».

De esta forma, el atacante puede obtener acceso no autorizado a los dispositivos afectados y luego usar esos puntos de entrada para conseguir acceso a otras redes. También pueden comprometer la disponibilidad, integridad o confidencialidad de los datos que se transmiten desde la red interna.

El investigador de seguridad Brendan Scarvell, que ha descubierto estas vulnerabilidades en routers TP-Link, también ha publicado detalles de dos vulnerabilidades de seguridad sin parchear que afectan a los routers TP-Link WR710N-V1-151022 y Archer-C5-V2-160201.

La primera de ellas, la CVE-2022-4499, podrían utilizarse para divulgar información y también puede realizar un ataque de canal lateral dirigido a una función utilizada para validar las credenciales., mientras que la segunda, la CVE-2022-4498, permite la ejecución remota de código.

RECOMENDACIONES:

- Para los usuarios de Netcomm y TP-Link estar pendientes de los parches de seguridad que se publicarán en sus páginas oficiales y actualizar lo antes posible para mitigar las vulnerabilidades.

Fuentes de información	▪ hxxps://thehackernews.com/2023/01/critical-security-vulnerabilities.html

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 017**	**Fecha: 19-01-2023** **Página 5 de 12**

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Oracle publica aviso de actualización de Parche Crítico (enero 2023) que afecta a varias familias de sus productos		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **Resumen:**

Oracle ha publicado una actualización **CRÍTICA** con parches para corregir vulnerabilidades que afectan a múltiples productos. Esta actualización de parche crítico contiene 327 nuevos parches de seguridad en las familias de productos de Oracle. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante realizar actividades maliciosas en las familias de productos de Oracle.

2. **Detalles:**

- Una actualización de parche crítico es una colección de parches para múltiples vulnerabilidades de seguridad. Estos parches abordan las vulnerabilidades en el código de Oracle y en los componentes de terceros incluidos en los productos de Oracle. Estos parches suelen ser acumulativos, pero cada aviso describe solo los parches de seguridad agregados desde el Aviso de actualización de parche crítico anterior. Por lo tanto, los avisos de actualización de parches críticos anteriores deben revisarse para obtener información sobre los parches de seguridad publicados anteriormente.
- Esta actualización de parche crítico contiene 327 nuevos parches de seguridad en las familias de productos de Oracle. Tenga en cuenta que una nota de MOS que resume el contenido de esta actualización de parche crítico y otras actividades de Oracle Software Security Assurance se encuentra en: Actualización de parche crítico de enero de 2023: Resumen ejecutivo y análisis .

3. **Productos afectados:**

- Big Data Spatial y Graph, versiones anteriores a 21.4.3, anteriores a 23.1.0;
- Plataforma basada en Enterprise Manager, versiones 13.4.0.0, 13.5.0.0;
- Enterprise Manager Ops Center, versión 12.4.0.0;
- Servidores Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S, versiones anteriores a XCP2411, anteriores a XCP3111, anteriores a XCP4011;
- GoldenGate Stream Analytics, versiones anteriores a 19.1.0.0.8;
- GoldenGate Veridata, versiones anteriores a 12.2.1.4.220831;
- JD Edwards EnterpriseOne Orchestrator, versiones anteriores a 9.2.7.2;
- JD Edwards EnterpriseOne Tools, versiones anteriores a 9.2.7.2;
- Motor de gestión en la nube, versión 22.1.0.0.0;
- Management Pack para Oracle GoldenGate, versiones anteriores a 12.2.1.2.221115;
- Herramientas y bibliotecas comunes de Middleware, versiones 12.2.1.4.0, 14.1.1.0.0;
- MySQL Cluster, versiones 7.4.38 y anteriores, 7.5.28 y anteriores, 7.6.24 y anteriores, 8.0.31 y anteriores;
- MySQL Connectors, versiones 8.0.31 y anteriores;
- MySQL Enterprise Monitor, versiones 8.0.32 y anteriores;
- MySQL Server, versiones 5.7.40 y anteriores, 8.0.31 y anteriores;
- MySQL Shell, versiones 8.0.31 y anteriores;
- MySQL Workbench, versiones 8.0.31 y anteriores;
- Administrador de acceso de Oracle, versión 12.2.1.4.0;
- Oracle Agile PLM, versión 9.3.6;
- Oracle AutoVue, versiones anteriores a 21.0.2.6;
- Oracle Banking Enterprise Default Management, versiones 2.6.2, 2.7.0, 2.7.1, 2.12.0;

- Oracle Banking Loans Servicing, versiones 2.8.0, 2.12.0;
- Oracle Banking Party Management, versión 2.7.0;
- Oracle Banking Platform, versiones 2.6.2, 2.7.1, 2.9.0, 2.12.0;
- Oracle BI Publisher, versiones 5.9.0.0.0, 6.4.0.0.0, 12.2.1.4.0;
- Oracle Business Intelligence Enterprise Edition, versiones 5.9.0.0.0, 6.4.0.0.0;
- Oracle Coherence, versiones 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0
- Búsqueda guiada de Oracle Commerce, versión 11.3.2;
- Ver lista completa aquí.

4. Solución:

- Oracle recomienda aplicar los parches de actualización de parche crítico, es posible reducir el riesgo de un ataque exitoso al bloquear los protocolos de red requeridos por un ataque;
- Para los ataques que requieren ciertos privilegios o acceso a ciertos paquetes, eliminar los privilegios o la capacidad de acceder a los paquetes de los usuarios que no los necesitan puede ayudar a reducir el riesgo de un ataque exitoso. Ambos enfoques pueden interrumpir la funcionalidad de la aplicación, por lo que Oracle recomienda encarecidamente que los clientes prueben los cambios en sistemas que no sean de producción. Ningún enfoque debe considerarse una solución a largo plazo, ya que ninguno corrige el problema subyacente.

Fuentes de información	▪ hxxps://www.oracle.com/security-alerts/cpujan2023.html ▪ hxxps://www.oracle.com/security-alerts/cpujan2023verbose.html ▪ hxxps://support.oracle.com/rs?type=doc&id=2834534.1 ▪ hxxps://www.oracle.com/security-alerts ▪ hxxps://www.oracle.com/security-alerts/advisorymatrixglossary.html

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 017**	**Fecha: 19-01-2023**
		Página 7 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en Red Hat Satellite		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **Resumen:**

Se ha reportado dos vulnerabilidades de severidad **ALTA** de tipo deserialización de datos no confiables e inyección de código en Red Hat Satellite. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino y comprometer por completo el sistema afectado.

2. **Detalles:**

- La vulnerabilidad de severidad **alta** registrada como CVE-2022-32224 de deserialización de datos no confiables, podría permitir que un usuario remoto ejecute código arbitrario en el sistema de destino. La vulnerabilidad existe debido a una validación de entrada insegura al procesar datos serializados en columnas en registros activos. Un acceso de escritura de usuario privilegiado remoto a la base de datos (por ejemplo, a través de la canalización de restauración) puede crear una columna especialmente diseñada y ejecutar código arbitrario en el sistema durante la restauración de la copia de seguridad.
- La vulnerabilidad de severidad **alta** registrada como CVE-2022-42889 de inyección de código, podría permitir que un atacante remoto ejecute código arbitrario en el sistema de destino. La vulnerabilidad existe debido a una interpolación de variables inseguras al procesar entradas que no son de confianza. Un atacante remoto puede enviar una entrada especialmente diseñada y ejecutar código arbitrario en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso completo del sistema vulnerable. Tenga en cuenta que la vulnerabilidad se denominó **Text4shell**.

3. **Productos afectados:**

- Red Hat Enterprise Linux for x86_64: 8.0;
- satellite-clone (Red Hat package): before 3.2.0-2.el8sat;
- satellite (Red Hat package): before 6.12.1-1.el8sat;
- rubygem-smart_proxy_container_gateway (Red Hat package): before 1.0.7-1.el8sat;
- rubygem-railties (Red Hat package): before 6.0.6-2.el8sat;
- rubygem-rails (Red Hat package): before 6.0.6-2.el8sat;
- rubygem-katello (Red Hat package): before 4.5.0.22-1.el8sat;
- rubygem-foreman_webhooks (Red Hat package): before 3.0.5-1.1.el8sat;
- rubygem-foreman_rh_cloud (Red Hat package): before 6.0.44-1.el8sat;
- rubygem-activesupport (Red Hat package): before 6.0.6-1.el8sat;
- rubygem-activestorage (Red Hat package): before 6.0.6-2.el8sat;
- rubygem-activerecord (Red Hat package): before 6.0.6-2.el8sat;
- rubygem-activemodel (Red Hat package): before 6.0.6-2.el8sat;
- rubygem-activejob (Red Hat package): before 6.0.6-2.el8sat;
- rubygem-actionview (Red Hat package): before 6.0.6-2.el8sat;
- rubygem-actiontext (Red Hat package): before 6.0.6-2.el8sat;
- rubygem-actionpack (Red Hat package): before 6.0.6-2.el8sat;
- rubygem-actionmailbox (Red Hat package): before 6.0.6-2.el8sat;
- rubygem-actioncable (Red Hat package): before 6.0.6-2.el8sat;
- foreman (Red Hat package): before 3.3.0.18-1.el8sat;
- candlepin (Red Hat package): before 4.1.18-1.el8sat.

4. Solución:

- Se recomienda actualizar los productos afectados con la última versión disponible que corrige estas vulnerabilidades.

Fuentes de información	▪ hxxp://access.redhat.com/errata/RHSA-2023:0261

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 017	Fecha: 19-01-2023
		Página 9 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de Phishing que suplanta a la entidad bancaria de Interbank.		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	G02
Clasificación temática familia	Fraude financiero		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que los ciberdelincuentes vienen llevando a cabo una campaña de envío masivo de correos electrónicos falsos, que pretenden ser de la entidad bancaria de Interbank, en el asunto del mensaje advierten ***"Le hacemos llegar una notificación debido a que su cuenta Interbank ha sido bloqueada, esto puede ser debido al ingreso sospechoso a su cuenta de terceros a través de banca por internet ",*** incluido un enlace oculto detrás del botón ***"Ingresa aquí"*** que, al ser pulsado, redirige a la víctima, a un sitio web falso de Interbank que simula ser el oficial, con el objetivo de robar las credenciales de acceso, información personal y/o financiera.

   - Proceso del ciberataque:

Figura 1. Correo inicial que llega a la víctima.

Figura 2. Solicitud para ingresar las credenciales de acceso (DNI, y clave web).

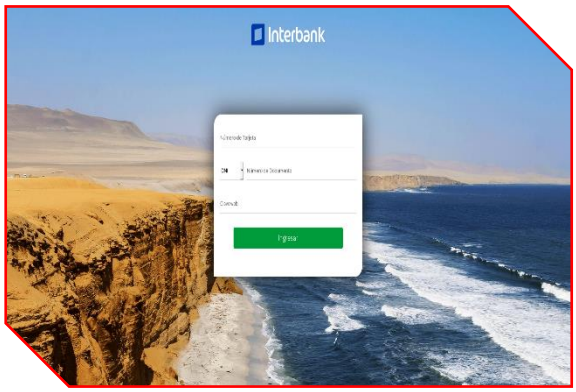


Figura 3. Seguidamente, parece validar los datos, pero en realidad la información fue robada por los ciberdelincuentes.

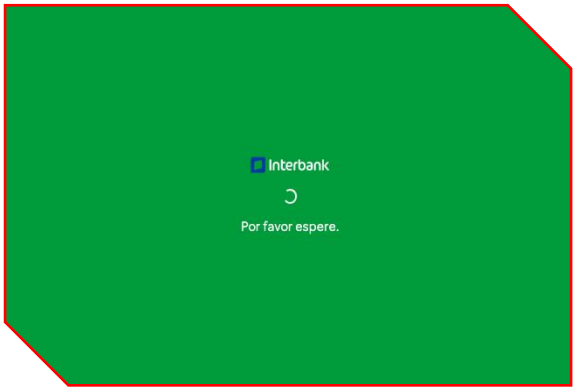
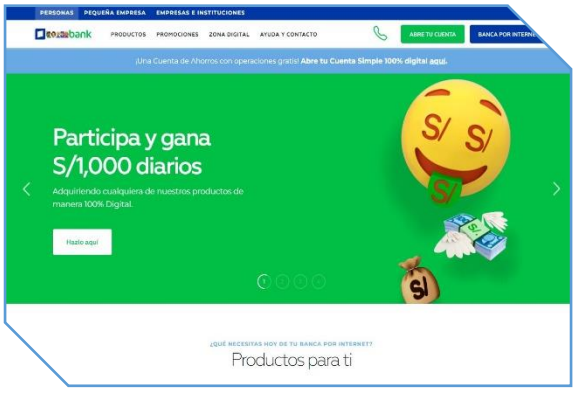


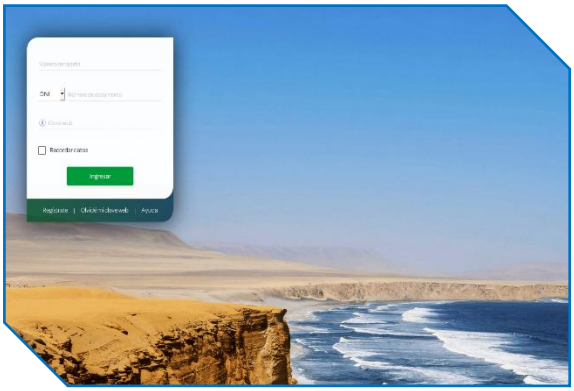
Figura 4. Al final, es redirigido al sitio web oficial Interbank, aludiendo un aparente error de autenticación.



- Comparación de los sitios web legítimo y falso del Banco Interbank:

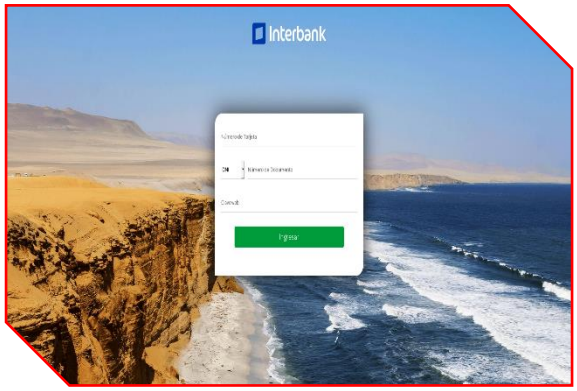
SITIO OFICIAL

URL: https://bancaporintenet.interbank.pe/login



SITIO FRAUDULENTO

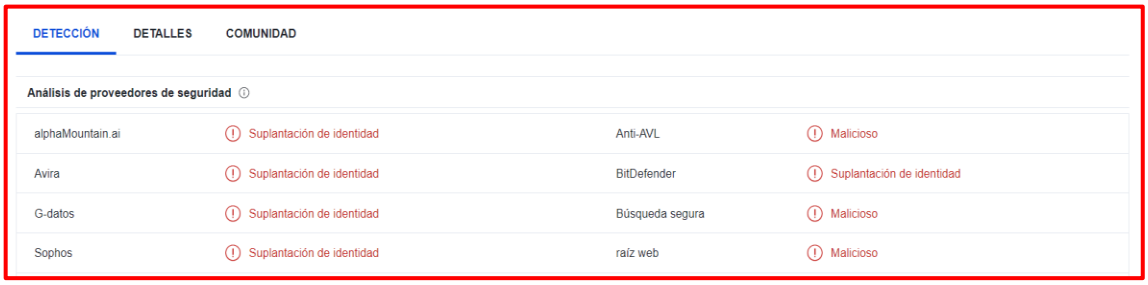
URL: hxxps[:]//alertas-movil-interbank[.]com



- Existe similitud en imagen, logotipo, fondo, color y escritura.
- Tiene certificado de seguridad de protocolo HTTPS.
- El dominio se hace pasar por el sitio oficial, pero no coinciden.

2. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

- Indicadores de compromisos:
  - **URL:** hXXps[:]//alertas-movil-interbank[.]com
  - **Dominio:** alertas-movil-interbank[.]com
  - **Dirección IP:** 45[.]88[.]202[.]115
  - **Código:** 200
  - **Longitud:** 6.11 KB
  - **SHA-256**: 176edfed461870dd89ebc2b709c3bd43354405e8f493aedf9cb04239b9b650ab

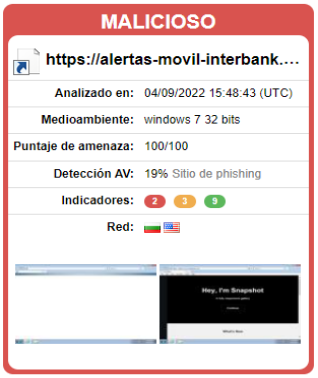


DETECCIÓN | DETALLES | COMUNIDAD

Análisis de proveedores de seguridad

alphaMountain.ai	Suplantación de identidad	Anti-AVL	Malicioso
Avira	Suplantación de identidad	BitDefender	Suplantación de identidad
G-datos	Suplantación de identidad	Búsqueda segura	Malicioso
Sophos	Suplantación de identidad	raíz web	Malicioso

- Otros resultados del análisis:



- Phishing:
    - Es un tipo de ataque de ingeniería social, que consiste en la utilización de envió masivo de email, los cuales se disfrazan para que parezcan proceder de una fuente de confianza. Estos emails están diseñados para engañar a las víctimas y conseguir que proporcionen información personal o financiera.

- Características de un Phishing:
    - Contiene errores ortográficos
    - No se respeta el formato (justificado)
    - Algunos emails son de alerta o urgencia
    - Tienen adjunto documento o URLs

3. Recomendaciones:

- Evitar ingresar los datos de autenticación en las URL que recibas por correo electrónico.
- Escribir directamente la URL de la entidad en el navegador.
- Sospechar de todos aquellos mensajes alarmantes que tengan tono de urgencia y contengan faltas de ortografía o erratas.
- No divulgar la información a amigos, familiares o terceros.
- Utilice un programa antivirus actualizado, ya que es la primera línea de defensa contra un ciberataque.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

Índice alfabético