



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

003-2026-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

Ciberatacantes utilizan falsas alertas de RTO Challan para propagar malware en Android 4

Vulnerabilidad en el software Cisco TelePresence Collaboration Endpoint y del software RoomOS. 6

Vulnerabilidad de carga arbitraria de archivos en Cisco Meeting Management. 7

Vulnerabilidad en productos de Broadcom Company..... 8

Vulnerabilidad en productos de Foxit Software Incorporated. 9

Vulnerabilidad de omisión crítica de autenticación en adaptadores Synectix LAN 232 TRIO al final de su vida útil. 10

Índice alfabético 11

| | | | |
|---|--|------------------------------|-------------------|
|  | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°003 | | Fecha: 04-02-2026 |
| | | | Página: 4 de 11 |
| Componente que reporta | CENTRO NACIONAL DE SEGURIDAD DIGITAL | | |
| Nombre de la alerta | Ciberatacantes utilizan falsas alertas de RTO Challan para propagar malware en Android | | |
| Tipo de Ataque | malware | Abreviatura | malware |
| Medios de propagación | Correo electrónico, redes sociales, entre otros | | |
| Código de familia | C | Código de Sub familia | C02 |
| Clasificación temática familia | Código Malicioso | | |

Descripción

1. ANTECEDENTES:

La investigación de GBHackers, basada en el análisis de Seqrite Labs, describe una campaña activa que suplanta notificaciones oficiales del Regional Transport Office (RTO) para “multas de tránsito pendientes” y que circula por WhatsApp/SMS con enlaces que descargan aplicaciones Android maliciosas fuera de Google Play; el objetivo es forzar la instalación de un APK que, mediante una cadena de infección de tres etapas, obtiene persistencia, comunica con una infraestructura Firebase de comando-y-control, exige permisos intrusivos (SMS, registros de llamadas, notificaciones y almacenamiento) y exfiltra identidad, OTPs bancarios, alertas de transacciones y metadatos del dispositivo hacia servidores de los atacantes, todo ello con técnicas anti-análisis, configuración remota y, en ciertos casos, minado furtivo que se activa con la pantalla bloqueada para pasar desapercibido.



Ilustración 1: Ciberatacantes utilizan falsas alertas de RTO Challan para propagar malware en Android

2. DETALLES:


La cadena maliciosa inicia con mensajes falsos de challan que introducen urgencia para que la víctima pulse un enlace y descargue un APK desde un alojamiento externo, evadiendo los controles de la tienda oficial; al ejecutarse, la Etapa 1 funciona como dropper y activa un criptominer cuando el dispositivo está bloqueado, preparando el terreno para el segundo componente; la Etapa 2 asegura persistencia ocultando el icono, registrando broadcast receivers, ejecutándose en segundo plano y conectando con Firebase para telemetría, configuración y C2, además de mantener su propio minado independiente; la Etapa 3 presenta una interfaz fraudulenta con identidad visual del RTO, solicita permisos de alto riesgo (SMS, llamadas, notificaciones, almacenamiento) y, tras concederse, recolecta PII, notificaciones bancarias y mensajes OTP, enviándolos en JSON a los servidores del actor; el uso de técnicas anti-análisis y la arquitectura modular confieren evasión y resiliencia, mientras que la distribución por plataformas de mensajería e instalación sideloaded amplían el alcance y evitan los controles de Google Play.


3. RECOMENDACIONES:

- Evitar toda instalación de APK desde enlaces de mensajería y deshabilitar “Fuentes desconocidas” en Android; si se recibió un aviso de challan, no instalar apps desde WhatsApp/SMS ni desde dominios no verificados, dado que la campaña se apoya precisamente en sideloading para eludir protecciones de Google Play.
- Verificar multas únicamente por canales oficiales abriendo el navegador y consultando manualmente el servicio gubernamental correspondiente; no seguir enlaces incrustados en mensajes que afirman urgencia o sanciones inminentes, el anzuelo principal señalado por la campaña.
- Revisar y limitar permisos: negar acceso a SMS, llamadas, notificaciones y archivos a cualquier app no oficial o recién instalada; estos permisos son los que el malware solicita para robar OTP y datos financieros.
- Monitorear señales de compromiso: consumo anómalo de batería/calor cuando la pantalla está bloqueada (posible criptominado), desaparición de íconos de apps y actividad inusual en notificaciones/mensajes; ante sospecha, aislar el dispositivo y proceder a la limpieza.
- Respuesta inmediata: si se instaló el APK, activar modo avión, retirar la SIM, cambiar credenciales bancarias y de correo desde otro equipo de confianza y restaurar a valores de fábrica para erradicar la persistencia y la conexión con Firebase/C2.

Fuente de Información:

- <https://gbhackers.com/fake-rto-challan/>

| | | | |
|---|--|---|-------------------|
|  | ALERTA DE SEGURIDAD DIGITAL N°058 | | Fecha: 04-02-2026 |
| | | | Página: 6 de 11 |
| Componente que reporta | DIRECCIÓN NACIONAL DE INTELIGENCIA | | |
| Nombre de la alerta | Vulnerabilidad en el software Cisco TelePresence Collaboration Endpoint y del software RoomOS. | | |
| Tipo de Ataque | Explotación de vulnerabilidades conocidas | Abreviatura | EVC |
| Medios de propagación | Redes sociales, SMS, correo electrónico, videos de internet, entre otros | | |
| Código de familia | H | Código de Sub familia | H01 |
| Clasificación temática familia | Intento de intrusión | | |
| Descripción | | | |
| <p>1. ANTECEDENTES:</p> <p>Cisco Systems, Inc. ha publicado una vulnerabilidad de severidad ALTA clasificada como CWE-1287: Validación incorrecta de un tipo de entrada específico que afecta al software Cisco TelePresence Collaboration Endpoint y del software RoomOS. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado provocar una condición de denegación de servicio (DoS) en un dispositivo afectado.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad alta identificada por MITRE como CVE-2026-20119 de tipo CWE-1287: Validación incorrecta de un tipo de entrada específico en el subsistema de representación de texto del software Cisco TelePresence Collaboration Endpoint (CE) y del software Cisco RoomOS, podría permitir a un atacante remoto no autenticado provocar la recarga del dispositivo afectado, lo que provocaría una DoS.</p> <p>Esta vulnerabilidad se debe a una validación insuficiente de la entrada recibida por un dispositivo afectado. Un atacante podría explotarla haciendo que el dispositivo afectado reproduzca texto manipulado, por ejemplo, una invitación a una reunión manipulada. Como se indica en la puntuación CVSS, no se requiere interacción del usuario, como aceptar la invitación a la reunión. Una explotación exitosa podría permitir al atacante provocar la recarga del dispositivo afectado, lo que provocaría una DoS.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> — Esta vulnerabilidad afecta al software Cisco TelePresence CE y al software Cisco RoomOS (versines anteriores a 10 y 11), independientemente de la configuración del dispositivo. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Cisco ha publicado actualizaciones de software que solucionan esta vulnerabilidad. No existen soluciones alternativas. | | | |
| Fuente de Información: | | <ul style="list-style-type: none"> • hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-tce-roomos-dos-9V9jrC2q | |

| | | | |
|---|---|------------------------------|-------------------|
|  | ALERTA DE SEGURIDAD DIGITAL N°059 | | Fecha: 04-02-2026 |
| | | | Página: 7 de 11 |
| Componente que reporta | DIRECCIÓN NACIONAL DE INTELIGENCIA | | |
| Nombre de la alerta | Vulnerabilidad de carga arbitraria de archivos en Cisco Meeting Management. | | |
| Tipo de Ataque | Explotación de vulnerabilidades conocidas | Abreviatura | EVC |
| Medios de propagación | Redes sociales, SMS, correo electrónico, videos de internet, entre otros | | |
| 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** clasificada como CWE-434: Carga sin restricciones de archivos con tipo peligroso en la función de administración de certificados de Cisco Meeting Management. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto autenticado cargue archivos arbitrarios, ejecute comandos arbitrarios y eleve privilegios a root en un sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como [CVE-2026-20098](#) de tipo CWE-434: Carga sin restricciones de archivos con tipo peligroso en la función de administración de certificados de Cisco Meeting Management, podría permitir a un atacante remoto autenticado cargue archivos arbitrarios, ejecute comandos arbitrarios y eleve privilegios a root en un sistema afectado. Esta vulnerabilidad se debe a una validación de entrada incorrecta en ciertas secciones de la interfaz de administración web.

Un atacante podría explotar esta vulnerabilidad enviando una solicitud HTTP manipulada a un sistema afectado. Una explotación exitosa podría permitir al atacante subir archivos arbitrarios al sistema afectado. Los archivos maliciosos podrían sobrescribir los archivos del sistema procesados por la cuenta raíz y permitir la ejecución de comandos arbitrarios con privilegios de root. Para explotar esta vulnerabilidad, el atacante debe tener credenciales válidas para una cuenta de usuario con al menos el rol de operador de video.


A. Productos afectados:


- Esta vulnerabilidad afecta a Cisco Meeting Management (versión 3.12 y anteriores), independientemente de la configuración del dispositivo.


3. RECOMENDACIONES:

- Cisco ha publicado actualizaciones de software que solucionan esta vulnerabilidad. No existen soluciones alternativas.

| | |
|-------------------------------|---|
| Fuente de Información: | <ul style="list-style-type: none"> • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmm-file-up-kY47n8kK |
|-------------------------------|---|

| | | | |
|---|--|---|-------------------|
|  | ALERTA DE SEGURIDAD DIGITAL N°060 | | Fecha: 04-02-2026 |
| | | | Página: 8 de 11 |
| Componente que reporta | DIRECCIÓN NACIONAL DE INTELIGENCIA | | |
| Nombre de la alerta | Vulnerabilidad en productos de Broadcom Company. | | |
| Tipo de Ataque | Explotación de vulnerabilidades conocidas | Abreviatura | EVC |
| Medios de propagación | Redes sociales, SMS, correo electrónico, videos de internet, entre otros | | |
| Código de familia | H | Código de Sub familia | H01 |
| Clasificación temática familia | Intento de intrusión | | |
| Descripción | | | |
| <p>1. ANTECEDENTES:</p> <p>Broadcom Company ha publicado una vulnerabilidad de severidad ALTA clasificada como CWE-209: Generación de un mensaje de error que contiene información confidencial que afecta a Brocade SANnav. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto autenticado con acceso a los logs de auditoría obtener la contraseña de la base de datos de SANnav.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad alta identificada por MITRE como CVE-2025-12773 de tipo CWE-209: Generación de un mensaje de error que contiene información confidencial que afecta a Brocade SANnav, podría permitir a un atacante remoto autenticado con acceso a los logs de auditoría obtener la contraseña de la base de datos de SANnav.</p> <p>Una vulnerabilidad en el registro del script “update-reports-purge-settings.sh” para Brocade SANnav anterior a 2.4.0a podría permitir la recopilación de la contraseña de la base de datos de SANnav en los registros de auditoría del sistema</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> – Brocade SANnav en versiones anteriores a 2.4.0a. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Actualizar Brocade SANnav versión 2.4.0a o superior para corregir el problema en el script de logging. • Revisar y limpiar los logs de auditoría existentes para eliminar cualquier contraseña expuesta. • Restringir el acceso a logs a usuarios autorizados y monitorear intentos de acceso no autorizados. | | | |
| Fuente de Información: | | <ul style="list-style-type: none"> • hxxps [://support[.]Broadcom[.]com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36847 | |

| | | | |
|---|--|---|-------------------|
|  | ALERTA DE SEGURIDAD DIGITAL N°061 | | Fecha: 04-02-2026 |
| | | | Página: 9 de 11 |
| Componente que reporta | DIRECCIÓN NACIONAL DE INTELIGENCIA | | |
| Nombre de la alerta | Vulnerabilidad en productos de Foxit Software Incorporated. | | |
| Tipo de Ataque | Explotación de vulnerabilidades conocidas | Abreviatura | EVC |
| Medios de propagación | Redes sociales, SMS, correo electrónico, videos de internet, entre otros | | |
| Código de familia | H | Código de Sub familia | H01 |
| Clasificación temática familia | Intento de intrusión | | |
| Descripción | | | |
| <p>1. ANTECEDENTES:</p> <p>Foxit Software Incorporated ha publicado una vulnerabilidad de severidad MEDIA clasificada como CWE-79: Neutralización incorrecta de la entrada durante la generación de páginas web (XSS o Cross-site Scripting) que afecta a la función de carga de archivos en Foxit PDF Editor Cloud (pdfonline.foxit.com). Requiere autenticación e interacción del usuario para explotación, impactando principalmente la confidencialidad mediante robo de sesiones o datos sensibles.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad media identificada por MITRE como CVE-2026-1591 de tipo CWE-79: Neutralización incorrecta de la entrada durante la generación de páginas web (XSS o Cross-site Scripting) que afecta a la función de carga de archivos en Foxit PDF Editor Cloud (pdfonline.foxit.com). Requiere autenticación e interacción del usuario para explotación, impactando principalmente la confidencialidad mediante robo de sesiones o datos sensibles.</p> <p>Una explotación exitosa de esta vulnerabilidad permite la ejecución de JavaScript arbitrario en el contexto del navegador de la víctima al visualizar la lista de archivos subidos en Foxit PDF Editor Cloud.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> – Foxit PDF Editor Cloud (pdfonline.foxit.com), todas las versiones anteriores al parche del 2026-02-01 o 2026-02-03. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Aplicar el parche lanzado por Foxit alrededor del 2026-02-01; • Validar y escapar todas las entradas de usuario en listas de archivos; • Restringir privilegios de carga y monitorear actividades de subida de archivos. Desactivar o limitar el acceso a pdfonline.foxit.com hasta parchear. | | | |
| Fuente de Información: | | <ul style="list-style-type: none"> • hxxps[:]//www[.]foxit[.]com/es/support/security-bulletins.html | |

| | | | |
|--|---|--|-------------------|
|  | ALERTA DE SEGURIDAD DIGITAL N°062 | | Fecha: 04-02-2026 |
| | | | Página: 10 de 11 |
| Componente que reporta | DIRECCIÓN NACIONAL DE INTELIGENCIA | | |
| Nombre de la alerta | Vulnerabilidad de omisión crítica de autenticación en adaptadores Synectix LAN 232 TRIO al final de su vida útil. | | |
| Tipo de Ataque | Explotación de vulnerabilidades conocidas | Abreviatura | EVC |
| Medios de propagación | Redes sociales, SMS, correo electrónico, videos de internet, entre otros | | |
| Código de familia | H | Código de Sub familia | H01 |
| Clasificación temática familia | Intento de intrusión | | |
| Descripción | | | |
| <p>1. ANTECEDENTES:</p> <p>Synectix ha publicado una vulnerabilidad de severidad CRÍTICA clasificada como CWE-306: Autenticación faltante para función crítica que afecta a los adaptadores seriales a Ethernet Synectix LAN 232 TRIO. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante no autenticado modifique configuraciones críticas del dispositivo o lo restablezca a la configuración de fábrica.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad crítica identificada por MITRE como CVE-2026-1633 de tipo CWE-306: Autenticación faltante para función crítica, se debe a que el adaptador serial a Ethernet de 3 puertos Synectix LAN 232 TRIO expone su interfaz de administración web sin requerir autenticación, lo que permite a los usuarios no autenticados modificar configuraciones críticas del dispositivo o restablecer el dispositivo a sus valores de fábrica. Esto significa que cualquiera con acceso a la red puede acceder sin contraseña.</p> <p>Al no existir barreras de autenticación, un atacante no necesita robar credenciales ni explotar código complejo. Simplemente necesita acceder a la dirección IP del dispositivo para tomar el control total.</p> <p>Los atacantes pueden acceder remotamente a la interfaz de administración web del dispositivo desde la red sin credenciales. Pueden modificar la configuración crítica del dispositivo y restablecerlo a la configuración de fábrica, lo que interrumpiría la comunicación serie-ethernet. Esto podría provocar la pérdida total de la funcionalidad del dispositivo y comprometer la integridad y disponibilidad de los sistemas que dependen de este adaptador.</p> <p>Los productos afectados deben considerarse al final de su vida útil, ya que Synectix ya no está en actividad y, por lo tanto, las correcciones, mitigaciones y actualizaciones de firmware no estarán disponibles.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> – Esta vulnerabilidad afecta a todas las versiones del adaptador serie a Ethernet Synectix LAN 232 TRIO de 3 puertos. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Los productos afectados deben considerarse al final de su vida útil, ya que Synectix ya no está en actividad y, por lo tanto, las correcciones, mitigaciones y actualizaciones de firmware no estarán disponibles. • Implementar la segmentación de red para restringir el acceso a la interfaz de administración web del dispositivo. • Limitar el acceso de red al adaptador únicamente a sistemas y redes de confianza. • Considerar usar un firewall o listas de control de acceso (ACL) para evitar conexiones de red no autorizadas a la interfaz de administración. • Supervisar el tráfico de red para detectar intentos de acceso sospechosos al dispositivo. • Contactar con Synectix para obtener actualizaciones de seguridad o recomendaciones de mitigación alternativas. | | | |
| Fuente de Información: | | <ul style="list-style-type: none"> • https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-034-04.json • https://www.cisa.gov/news-events/ics-advisories/icsa-26-034-04 | |

Índice alfabético

malware 4

Explotación de vulnerabilidades conocidas 6,7,8,9,10