SecurityScorecard

INFORME DETALLADO

Scorecard para Formiik

Generado **6 de diciembre de 2021**
por David Rodriguez (davrodriguez@bancow.com.co), Banco W

Acerca de este informe

Este informe es una captura puntual de este Scorecard desde las 16:58:42 UTC del 6 de diciembre de 2021. No debe confundirse con un resultado de prueba de penetración ni con una evaluación final.

Obtenga una visión global con SecurityScorecard

SecurityScorecard ofrece control automático continuo, informes de historial, exportaciones de datos en formato CSV y muchas más funciones que ayudarán a los equipos de seguridad a proteger sus organizaciones. Para obtener acceso gratuito al Scorecard de su organización, cree una cuenta hoy mismo en bit.ly/2P8okyb.

Obtenga hoy mismo más información sobre SecurityScorecard en bit.ly/2xXNg4N.

¿Qué es SecurityScorecard?

SecurityScorecard es un servicio de calificación (Score) de seguridad que utiliza un sencillo sistema de calificación de la A (puntuación máxima) a la F (puntuación mínima) para calificar la seguridad general de las empresas, así como 10 importantes factores de riesgo. Una empresa con una calificación C, D o F tiene 5,4 veces más probabilidades de sufrir una filtración importante que empresas con una calificación A o B[1]. Ciertos factores de riesgo, como la seguridad de las aplicaciones y la cadencia de la aplicación de revisiones, tienen aún más efecto sobre la probabilidad de sufrir una filtración. Si se obtiene una F en lugar de una A en dichos factores, la probabilidad de que se produzca una filtración de datos o un ataque es diez veces mayor.

Obtenga más información sobre el sistema de Score de SecurityScorecard en bit.ly/2zMLSmW.

[1] "La investigación de SecurityScorecard puede ayudarle a detectar una fuga de datos antes de que esta ocurra" (https://bit.ly/2yc0JVN)

Próximos pasos: Conseguir (A)

1. Cree una cuenta

Este archivo incluye muchos detalles, pero recuerde: se refiere solo a un momento puntual. Cree una cuenta si quiere obtener acceso completo y gratuito al Scorecard completo de su organización, además de auto-monitoreo continuo, informes de historial, exportaciones de datos en formato CSV y otras muchas cosas.

2. Valide su huella digital

Una vez que tenga una cuenta, revise la huella digital de su empresa, los activos que SecurityScorecard considera potencialmente atribuibles a su empresa, que afectan a las calificaciones de su Scorecard. Solicite la eliminación o adición de IP según sea necesario.

3. Examine los hallazgos sobre los problemas

Investigue junto con sus equipos el contenido de su tarjeta de puntuación. La postura de seguridad de su empresa saldrá ganando si se identifican cabos sueltos de los que antes no eran conscientes.

4. Corrija los problemas y mejore su Score

Tanto si ha aplicado una corrección como si ha encontrado activos que no pertenecen a su empresa o desea compartir información sobre los controles de compensación, puede informarnos solucionando los problemas identificados y enviándolos para que aprobemos su resolución. Nuestro equipo de suporte se encarga de gestionar las resoluciones y resolverá cualquier asunto pendiente en un plazo de tres días hábiles. Corrija los problemas en la propia plataforma o envíe un correo electrónico a support@securityscorecard.com.

Estamos aquí para ayudarle

La plataforma SecurityScorecard se basa en la transparencia y la colaboración. Nuestro equipo de Asistencia para fiabilidad del cliente proporciona servicios de corrección y resolución sin cargo alguno y estaremos encantados de trabajar con usted y sus clientes para resolver cualquier problema. Si necesita ayuda en cualquier momento, contacte con nosotros enviando un correo electrónico a support@securityscorecard.io.

Visión general del Scorecard

B

Formiik

Puntuación de seguridad: 82

DOMINIO: formiik.com

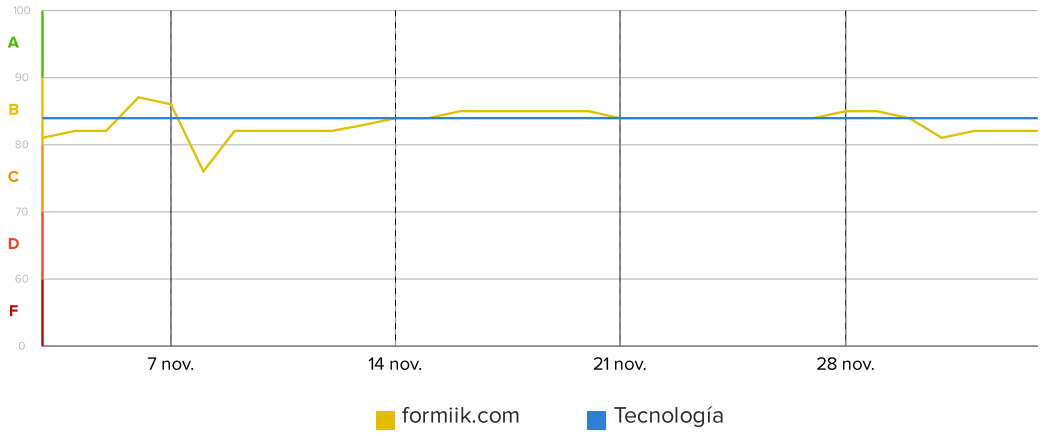
SECTOR: TECNOLOGÍA

Factores de Riesgo

C	77	SEGURIDAD DE APLICACIONES	5 INCIDENCIAS		
A	100	CUBIT SCORE	0 NINGUNA INCIDENCIA		
A	90	ESTADO DE DNS	1 INCIDENCIA		
A	100	SEGURIDAD DEL ENDPOINT	0 NINGUNA INCIDENCIA		
A	100	HACKER CHATTER	0 NINGUNA INCIDENCIA		
A	100	REPUTACIÓN DE IP	0 NINGUNA INCIDENCIA		
A	100	FILTRACIÓN DE INFORMACIÓN	0 NINGUNA INCIDENCIA		
F	53	SEGURIDAD DE RED	5 INCIDENCIAS		
C	73	CADENCIA DE APLICACIÓN DE REVISIONES	4 INCIDENCIAS		
A	100	INGENIERÍA SOCIAL	1 INCIDENCIA		

Historial del Score en los últimos 30 días

En el siguiente cuadro se muestra la evolución de la clasificación de seguridad relativa de la empresa a lo largo del tiempo. Los picos en la puntuación de rendimiento representan mejoras en la seguridad general, corrección de incidencias abiertas y mejoras en la protección de la infraestructura de la empresa. Las caídas reflejan la introducción de configuraciones erróneas en el sistema o la aplicación, o bien actividades prolongadas de malware.



Elementos de acción

FACTOR	GRAVEDAD	IMPACTO EN EL SCORE	PROBLEMAS DETECTADOS
Seguridad de Aplicaciones	!!	-1.7	El sitio web no implementa las prácticas recomendadas de HSTS. Incluso si un sitio web está protegido con HTTPS, la mayoría de los navegadores intentarán conectarse primero a la versión HTTP del sitio web a menos que se especifique explícitamente. En ese momento, los visitantes del sitio web son vulnerables a un atacante de tipo “man in the middle” que puede impedirles llegar a la versión HTTPS del sitio web que pretendían visitar y, en su lugar, desviarlos a un sitio web malintencionado. El encabezado HSTS (expandir) garantiza que, después de la visita inicial de un usuario al sitio web, no sean susceptibles a este ataque de intermediario, porque se conectarán inmediatamente al sitio web protegido por HTTPS.
	!!	-2.0	Falta la política de seguridad de contenido (PSC). Una directiva de política de seguridad de contenido (PSC) indica a un navegador web desde qué ubicaciones puede cargar recursos al renderizar una página web. Esto ayuda a evitar la inyección de recursos erróneos o malintencionados en una página web (y su posterior ejecución por parte del navegador de un usuario).
Estado de DNS	!!	-0.5	Falta el registro SPF. Se ha detectado que falta un registro SPF para un dominio.
Seguridad de Red	!!	-3.5	El certificado ha caducado. Los certificados caducados impiden que los clientes TLS se conecten a los servidores.
	!!	-5.1	Remote Access Service Observed. We observed a remote access service or device publicly exposed.
	!!	-2.6	SSH admite algoritmos MAC débiles. Se ha detectado un algoritmo de código de autenticación de mensajes (MAC) débil.
	!!	-3.0	SSH admite cifrado débil. Se ha detectado un cifrado débil.
Cadencia de aplicación de revisiones	!!!	-0.4	Vulnerabilidad de gravedad alta en la última observación. Hemos observado una vulnerabilidad de gravedad alta durante nuestro último análisis, que aún puede estar expuesta públicamente.
	!!!	-0.5	Patching Cadence (Secuencia de parches) a VEC de gravedad alta. High severity vulnerability seen on network more than 45 days after CVE was published.
	!!	-0.5	Vulnerabilidad de gravedad media en la última observación. Durante nuestro último análisis, hemos observado una vulnerabilidad de gravedad media, que aún puede estar expuesta públicamente.
	!!	-0.5	Patching Cadence (Secuencia de parches) a VEC de gravedad media. Medium severity vulnerability seen on network more than 90 days after CVE was published.

C 77 SEGURIDAD DE APLICACIONES

El módulo Web Application Security (Seguridad de Aplicaciones) utiliza inteligencia sobre amenazas entrantes por vulnerabilidades conocidas, que se identifican mediante bases de datos VEC “whitehat”, bases de datos de vulnerabilidades “blackhat” y hallazgos importantes indexados por los principales motores de búsqueda. El módulo ingiere datos de múltiples conjuntos de datos públicos, fuentes de terceros y un motor interno de indexación y agregación patentado.
La puntuación determina la probabilidad de una próxima infracción de la aplicación web y comprueba si hay algún código de "defacement" (desfiguración) existente. La presencia de aplicaciones vulnerables, versiones obsoletas y desfiguraciones activas se utiliza para calcular la puntuación general.

GRAVEDAD ALTA

No hay Problemas de gravedad alta para Application Security

GRAVEDAD MEDIA

El sitio web no implementa las prácticas recomendadas de HSTS	4
Falta la política de seguridad de contenido (PSC)	4

GRAVEDAD BAJA

No hay Problemas de gravedad baja para Application Security

POSITIVA

No hay Señales positivos para Application Security

INFORMATIVOS

El sitio web no implementa las prácticas recomendadas de protección X-XSS	1
Website Copyright is Not Current	1
Implementación insegura de la integridad de los recursos secundarios (SRI)	1

El sitio web no implementa las prácticas recomendadas de protección X-XSS

Si no se establece explícitamente la protección X-XSS, los clientes que vean un sitio web corren el riesgo de sufrir ataques de scripts en sitios cruzados (XSS) reflejados.

Descripción
El encabezado de respuesta HTTP X-XSS-Protection es una característica de Internet Explorer, Chrome y Safari que impide que las páginas se carguen cuando detectan ataques de scripts en sitios cruzados (XSS) reflejados. Aunque estas protecciones son en gran medida innecesarias en los navegadores modernos cuando los sitios web implementan una fuerte política de seguridad de contenido que deshabilita el uso de JavaScript en línea (“unsafe-inline”), todavía pueden proporcionar protecciones para los usuarios de navegadores web antiguos que aún no admiten PSC. Sin estas protecciones, un atacante puede enviar a sus víctimas URL malintencionadas que inyecten código en el sitio web.

Recomendación
Añada el siguiente encabezado a las respuestas de este sitio web: “X-XSS-Protection: 1; mode=block”

1 resultado

ANÁLISIS	DOMINIO	SCHEME	OBSERVACIONES	FECHA DE ÚLTIMA OBSERVACIÓN	FINAL URL
x_xss_protection_missing	formiik.com	https	97	3/12/2021 1:15:52	https://formiik.com/?ao=1

Website Copyright is Not Current

We observed copyright on a public-facing website in your network that is not current.

Descripción

Recomendación

A website with older copyright can be associated with security risks. It may indicate a lack of attention to the maintenance of the site. For example, parts of a site that have not changed for an extended period, such as a data intake form, may have components that require security updates.

Review all of your site content and code regularly to ensure that copyrights, code, and other content remain up to date.

1 resultado

URL	FECHA DE ÚLTIMA OBSERVACIÓN
formiik.com Evidencia: [object Object]	22/11/2021 11:45:34

El sitio web no implementa las prácticas recomendadas de HSTS

-1.7 IMPACTO EN EL SCORE

Incluso si un sitio web está protegido con HTTPS, la mayoría de los navegadores intentarán conectarse primero a la versión HTTP del sitio web a menos que se especifique explícitamente. En ese momento, los visitantes del sitio web son vulnerables a un atacante de tipo “man in the middle” que puede impedirles llegar a la versión HTTPS del sitio web que pretendían visitar y, en su lugar, desviarlos a un sitio web malintencionado. El encabezado HSTS (expandir) garantiza que, después de la visita inicial de un usuario al sitio web, no sean susceptibles a este ataque de intermediario, porque se conectarán inmediatamente al sitio web protegido por HTTPS.

Descripción
HTTP Strict Transport Security (HTTP con seguridad de transporte estricta) es un encabezado HTTP que indica a los clientes (por ejemplo, navegadores web) que solo se conecten a un sitio web mediante conexiones HTTPS cifradas. Los clientes que respeten este encabezado actualizarán automáticamente todos los intentos de conexión de HTTP a HTTPS.
Una vez que un cliente recibe el encabezado HSTS en su primera visita al sitio web, las conexiones futuras a ese sitio web están protegidas frente a ataques de tipo “man in the middle” que intentan la degradación a una conexión HTTP no cifrada.
El navegador dará por caducado el encabezado HTTP Strict Transport Security después del número de segundos configurado en el atributo de antigüedad máxima.

Recomendación
Toda aplicación web (y cualquier URL por la que se pase para llegar al sitio web mediante redireccionamientos) debe configurar el encabezado HSTS para que permanezca en vigor durante al menos 12 meses (31 536 000 segundos). Igualmente se recomienda configurar la directiva “includeSubDomains” para que las solicitudes a subdominios también se actualicen automáticamente a HTTPS.
Un encabezado HSTS aceptable sería:
Strict-Transport-Security: max-age=31536000; includeSubDomains;

4 resultados

ANÁLISIS	DOMINIO	SCHEME	OBSERVACIONES	FECHA DE ÚLTIMA OBSERVACIÓN	FINAL URL
hsts_missing_subdomain	formiik.com	https	42	3/12/2021 6:42:34	https://app.formiik.com/
no_hsts	formiik.com	https	97	3/12/2021 1:15:52	https://formiik.com/?ao=1
hsts_missing_subdomain	formiik.com	https	2	3/12/2021 0:04:26	https://dev.formiik.com/
hsts_missing_subdomain	formiik.com	https	4	2/12/2021 10:06:16	https://services.formiik.com/

Implementación insegura de la integridad de los recursos secundarios (SRI)

La integridad de los recursos secundarios (SRI) es una característica de seguridad que permite a los navegadores verificar que los archivos que recuperan (por ejemplo, de una CDN) se entregan sin manipulación inesperada. Su funcionamiento se basa en permitir que los elementos del sitio web proporcionen un hash criptográfico que debe coincidir con un archivo recuperado.

Descripción

Recomendación

Muchos sitios web que dependen de archivos de hoja de estilo JavaScript y CSS alojarán estos recursos estáticos en organizaciones externas (normalmente CDN) para mejorar los tiempos de carga del sitio web. Lamentablemente, si una de estas organizaciones externas se ve comprometida, los archivos JavaScript y CSS que aloja también pueden verse comprometidos y utilizarse para enviar código malintencionado al sitio web original.
La integridad de los recursos secundarios (SRI) es una forma de que el propietario de un sitio web añada un valor de suma de comprobación a todos los archivos alojados externamente que utiliza el navegador, para verificar que los archivos cargados desde organizaciones externas no se han modificado.

Asegúrese de que todos los elementos del sitio web (es decir, <script> y <link>) que cargan hojas de estilo JavaScript y CSS alojadas en organizaciones externas contengan la directiva “integrity” con una suma de comprobación válida.
Ejemplo:
<script src="https://example.com/example-framework.js" integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC" crossorigin="anonymous"></script>

1 resultado

DOMINIO	SCHEME	OBSERVACIONES	FECHA DE ÚLTIMA OBSERVACIÓN
formiik.com	https	81	3/12/2021 1:15:52

Falta la política de seguridad de contenido (PSC)

-2.0 IMPACTO EN EL SCORE

Una directiva de política de seguridad de contenido (PSC) indica a un navegador web desde qué ubicaciones puede cargar recursos al renderizar una página web.
Esto ayuda a evitar la inyección de recursos erróneos o malintencionados en una página web (y su posterior ejecución por parte del navegador de un usuario).

Descripción
La Política de seguridad de contenido proporciona una valiosa red de seguridad que protege su sitio web frente a ataques malintencionados de scripts de sitios (XSS). Una directiva bien configurada impedirá que un atacante trate de insertar su código o referencias a otro contenido malintencionado en su sitio web.
Sin una política de seguridad de contenido, es fácil que los desarrolladores de sitios web cometan errores que permitan a un atacante inyectar contenido que cambie la forma en que el sitio web se comporta.

Recomendación
Habilite los encabezados PSC a través de la configuración de su servidor web.

4 resultados

DOMINIO	SCHEME	OBSERVACIONES	FECHA DE ÚLTIMA OBSERVACIÓN	FINAL URL
formiik.com	https	42	3/12/2021 6:42:34	https://app.formiik.com/
formiik.com	https	97	3/12/2021 1:15:52	https://formiik.com/?ao=1
formiik.com	https	2	3/12/2021 0:04:26	https://dev.formiik.com/
formiik.com	https	4	2/12/2021 10:06:16	https://services.formiik.com/

CUBIT SCORE

Este módulo patentado mide distintos problemas de seguridad que una empresa podría tener. Por ejemplo, comprobamos las bases de datos públicas sobre inteligencia de amenazas en busca de direcciones IP que hayan sido señaladas. Estas configuraciones erróneas pueden presentar una alta vulnerabilidad y podrían causar daños significativos a la privacidad de sus datos e infraestructura.

GRAVEDAD ALTA

No hay Problemas de gravedad alta para Cubit Score

GRAVEDAD MEDIA

No hay Problemas de gravedad media para Cubit Score

GRAVEDAD BAJA

No hay Problemas de gravedad baja para Cubit Score

POSITIVA

No hay Señales positivos para Cubit Score

INFORMATIVOS

No hay Señales informativos para Cubit Score

No se encontró ningún problema

A 90 ESTADO DE DNS

El módulo DNS Health (Salud del DNS) mide el estado y la configuración de los ajustes DNS de una empresa. Valida que no se hayan producido eventos maliciosos en el historial DNS pasivo de la red de la empresa, ayuda a validar que los servidores de correo tengan la protección adecuada para evitar la falsificación (o "spoofing") y permite verificar que los servidores DNS estén configurados correctamente.

GRAVEDAD ALTA	GRAVEDAD MEDIA		GRAVEDAD BAJA	POSITIVA
No hay Problemas de gravedad alta para DNS Health	Falta el registro SPF	1	No hay Problemas de gravedad baja para DNS Health	No hay Señales positivos para DNS Health

INFORMATIVOS

No hay Señales informativos para DNS Health

Falta el registro SPF

Se ha detectado que falta un registro SPF para un dominio.

-0.5 IMPACTO EN EL SCORE

Descripción
El método Sender Policy Framework (SPF) es una técnica simple pero eficaz de validación de correo electrónico diseñada para detectar la falsificación (o "spoofing") de correo electrónico. Un registro SPF es un mecanismo que permite a un servidor de correo electrónico receptor validar que el correo electrónico entrante de un dominio en particular proviene de un servidor autorizado para enviar correo electrónico en nombre de ese dominio en particular. La lista de hosts de envío autorizados para un dominio se publica como un registro del Sistema de nombres de dominio (DNS) para ese dominio en forma de un registro TXT con formato especial. Se requiere un registro SPF para la prevención del correo electrónico falsificado y el control antispam.

Recomendación
Cree un registro válido de Sender Policy Framework (SPF). Asegúrese de configurar el registro DNS de SPF para verificar la sintaxis y los servidores MTA. Pruebe la configuración para asegurarse de que sea válida, mediante la comprobación del encabezado de un correo electrónico entrante en busca de “spf=pass”. Permita el almacenamiento en caché DNS durante las pruebas; puede tardar hasta 48 horas en propagarse completamente a través de Internet. La naturaleza del protocolo SMTP no permite la prevención total de la falsificación ("spoofing") de correos electrónicos; no obstante, el encabezado SPF revelará si el correo electrónico es auténtico.

1 resultado

DOMINIO	FECHA DE ÚLTIMA OBSERVACIÓN
formiik.com	3/12/2021 7:09:20

A 100 SEGURIDAD DEL ENDPOINT

El módulo Endpoint Security (Seguridad del Endpoint) realiza un seguimiento de los puntos de identificación que se extraen de los metadatos relacionados con el sistema operativo, el navegador web y los complementos activos relacionados. La información recopilada permite a las empresas identificar versiones obsoletas de estos puntos de datos que pueden dar lugar a ataques de explotación del lado del cliente.

GRAVEDAD ALTA

No hay Problemas de gravedad alta para Endpoint Security

GRAVEDAD MEDIA

No hay Problemas de gravedad media para Endpoint Security

GRAVEDAD BAJA

No hay Problemas de gravedad baja para Endpoint Security

POSITIVA

No hay Señales positivos para Endpoint Security

INFORMATIVOS

No hay Señales informativos para Endpoint Security

No se encontró ningún problema

A 100 HACKER CHATTER

El módulo Hacker Chatter de SecurityScorecard es un sistema automatizado de recopilación y agregación para el análisis de múltiples flujos de charla de piratas informáticos en sitios clandestinos. Continuamente se supervisan, recopilan y agregan foros, IRC, redes sociales y otros repositorios públicos de conversaciones de la comunidad de piratas informáticos para localizar menciones a nombres de empresas y sitios web. La puntuación de Hacker Chatter es una clasificación informativa de indicadores basada en la cantidad de indicadores detectados por los sensores de recopilación.

GRAVEDAD ALTA

No hay Problemas de gravedad alta para Hacker Chatter

GRAVEDAD MEDIA

No hay Problemas de gravedad media para Hacker Chatter

GRAVEDAD BAJA

No hay Problemas de gravedad baja para Hacker Chatter

POSITIVA

No hay Señales positivos para Hacker Chatter

INFORMATIVOS

No hay Señales informativos para Hacker Chatter

No se encontró ningún problema

A 100 REPUTACIÓN DE IP

Los módulos IP Reputation y Malware Exposure (Reputación IP y Exposición al malware) utilizan la infraestructura de sistemas “sinkhole” de SecurityScorecard, así como una combinación de fuentes de malware OSINT y asociaciones de intercambio de datos de inteligencia de amenazas de terceros. El sistema “sinkhole” de SecurityScorecard ingiere millones de señales de malware procedentes de infraestructuras de comando y control (C2) de todo el mundo. Los datos entrantes se procesan y atribuyen a las empresas. La cantidad y duración de las infecciones por malware se utilizan como factor determinante para calcular el indicador clave de amenaza del módulo Exposición al malware.

GRAVEDAD ALTA

No hay Problemas de gravedad alta para IP Reputation

GRAVEDAD MEDIA

No hay Problemas de gravedad media para IP Reputation

GRAVEDAD BAJA

No hay Problemas de gravedad baja para IP Reputation

POSITIVA

No hay Señales positivos para IP Reputation

INFORMATIVOS

No hay Señales informativos para IP Reputation

No se encontró ningún problema

A 100 FILTRACIÓN DE INFORMACIÓN

Este módulo Information Leak (Filtración de información) hace uso de las capacidades de supervisión de charlas y supervisión web profunda para identificar las credenciales comprometidas que los piratas informáticos están haciendo circular. Se trata de filtraciones masivas de datos anunciadas públicamente, así como filtraciones e intercambios más pequeños entre piratas informáticos.

GRAVEDAD ALTA

No hay Problemas de gravedad alta para Information Leak

GRAVEDAD MEDIA

No hay Problemas de gravedad media para Information Leak

GRAVEDAD BAJA

No hay Problemas de gravedad baja para Information Leak

POSITIVA

No hay Señales positivos para Information Leak

INFORMATIVOS

No hay Señales informativos para Information Leak

No se encontró ningún problema

F 53 SEGURIDAD DE RED

El módulo Network Security (Seguridad de Red) comprueba los conjuntos de datos públicos en busca de pruebas de puertos abiertos de alto riesgo o inseguros dentro de la red de la empresa. Los puertos inseguros a menudo se pueden explotar para permitir que un atacante eluda el proceso de inicio de sesión u obtenga un acceso profundo al sistema. Si está mal configurado, el puerto abierto puede actuar como punto de entrada entre la estación de trabajo de un pirata informático y su red interna.

GRAVEDAD ALTA

No hay Problemas de gravedad alta para Network Security

GRAVEDAD MEDIA

El certificado ha caducado	2
Remote Access Service Observed	2
SSH admite algoritmos MAC débiles	1
SSH admite cifrado débil	1

GRAVEDAD BAJA

No hay Problemas de gravedad baja para Network Security

POSITIVA

No hay Señales positivos para Network Security

INFORMATIVOS

Cloud Provider Service Used	4

El certificado ha caducado

Los certificados caducados impiden que los clientes TLS se conecten a los servidores.

-3.5 IMPACTO EN EL SCORE

Descripción
When a Certificate Authority (CA) issues a certificate, they embed two dates: the date at which the certificate starts being valid, and the date at which the certificate stops being valid. If a TLS client (e.g., web browser) connects to a TLS server (e.g., website) and receives a certificate that is expired, then the TLS client will refuse to connect.
Certificates are digital assets that require renewal or decommissioning on a schedule.

Recomendación
Services presenting expired certificates should cause noticeable failures, so confirm the service is still in use. If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.
Evaluate the organization's certificate management policy to ensure that certificates are renewed or decommissioned prior to their expiration date.

2 resultados

TARGET	SHA-256 FINGERPRINT	OBSERVACIONES	FECHA DE ÚLTIMA OBSERVACIÓN
score.formiik.com	c5cdcce7cf0162e6cb5f1cf5fb822265f8d8 12 b85c9e296aed6dfae263f3e9b36a		16/11/2021 14:59:14
Evidencia: Sat Oct 13 2018 23:59:59 GMT+0000 (Coordinated Universal Time)			
200.53.143.104	c5cdcce7cf0162e6cb5f1cf5fb822265f8d8 18 b85c9e296aed6dfae263f3e9b36a		9/11/2021 5:08:18
Evidencia: Sat Oct 13 2018 23:59:59 GMT+0000 (Coordinated Universal Time)			

Remote Access Service Observed

We observed a remote access service or device publicly exposed.

-5.1 IMPACTO EN EL SCORE

Descripción
Remote access services allow users to reach endpoints on a network (separate of RDP/X11/VNC) with Microsoft Windows-Based Terminal (WBT). This server is used for Windows Remote Desktop and Remote Assistance connections, or router login services, such as TP-LINK/CPE/ActionTec TR-069. These devices can be a security risk and enable an entry point into a network by attackers.

Recomendación
This issue type concerns a remote access service, such as a router providing a remote login service, or a Windows server providing a remote assistance service. Examine devices on a case-by-case basis, restrict access to these devices to either authorized VPN connections or IP restrictions.

2 resultados

NOMBRE DE PRODUCTO	DIRECCIÓN IP	PUERTO	FECHA DE ÚLTIMA OBSERVACIÓN
Microsoft WBT Server	20.97.57.213	3389	30/11/2021 19:14:30
	20.97.57.213	3389	8/11/2021 4:59:24

SSH admite algoritmos MAC débiles

Se ha detectado un algoritmo de código de autenticación de mensajes (MAC) débil.

-2.6 IMPACTO EN EL SCORE

Descripción
El servidor SSH está configurado para admitir algoritmos MD5. La solidez criptográfica depende del tamaño de la clave y del algoritmo utilizado. En lugar de MD5 se deben usar algoritmos MAC modernos como SHA1 o SHA2.

Recomendación
Configure el servidor SSH para desactivar el uso de MD5.

1 resultado

DIRECCIÓN IP	PUERTO	FECHA DE ÚLTIMA OBSERVACIÓN
200.53.143.104	22	5/11/2021 16:04:31
Evidencia: hmac-md5-etm@openssh.com		

Cloud Provider Service Used

We discovered that you use a cloud provider service to host your web site or applications.

Descripción
There is no security risk associated with using a cloud provider service, such as AWS or Google Cloud, to host your web site or applications. It is an increasingly common business solution that places considerable computing resources and fault tolerance at your disposal, without the maintenance overhead. Your customers or partners may want to know if you rely on a cloud provider service because they then also rely on that vendor and the dependability of their services. IPs associated with the cloud provider service are listed in your inventory.

Recomendación
Identification of a cloud provider service could be useful information to your customers and partners, and there is no recommended action.

4 resultados

NOMBRE DE PRODUCTO	VERSIÓN DE PRODUCTO	DIRECCIÓN IP	PUERTO	FECHA DE ÚLTIMA OBSERVACIÓN
Microsoft HTTPAPI httpd	2.0	20.97.57.213	8084	8/11/2021 4:59:24
Microsoft HTTPAPI httpd	2.0	20.97.57.213	80	8/11/2021 4:59:24
		20.97.57.213	8089	8/11/2021 4:59:24
		20.97.57.213	3389	8/11/2021 4:59:24

SSH admite cifrado débil

Se ha detectado un cifrado débil.

-3.0 IMPACTO EN EL SCORE

Descripción
El servidor SSH está configurado para admitir algoritmos cifrados en modo Arcfour o Cipher Block Chaining (CBC). SSH se puede configurar para utilizar el cifrado en modo Counter (CTR) en lugar de CBC. Conviene deshabilitar el uso de algoritmos Arcfour.

Recomendación
Configure el servidor SSH para deshabilitar los cifrados Arcfour y CBC.

1 resultado

DIRECCIÓN IP	PUERTO	FECHA DE ÚLTIMA OBSERVACIÓN
200.53.143.104	22	5/11/2021 16:04:31
Evidencia: arcfour256		

C 73 CADENCIA DE APLICACIÓN DE REVISIONES

El módulo Patching Cadence (Secuencia de parches) analiza la rapidez con la que una empresa reacciona a las vulnerabilidades para medir las prácticas de aplicación de revisiones. Analizamos la velocidad a la que una empresa necesita remediar y aplicar revisiones en comparación con empresas similares.

GRAVEDAD ALTA

Vulnerabilidad de gravedad alta en la última observación	2
Patching Cadence (Secuencia de parches) a VEC de gravedad alta	2

GRAVEDAD MEDIA

Vulnerabilidad de gravedad media en la última observación	28
Patching Cadence (Secuencia de parches) a VEC de gravedad media	28

GRAVEDAD BAJA

No hay Problemas de gravedad baja para Patching Cadence

POSITIVA

No hay Señales positivos para Patching Cadence

INFORMATIVOS

No hay Señales informativos para Patching Cadence

Vulnerabilidad de gravedad alta en la última observación

-0.4 IMPACTO EN EL SCORE

Hemos observado una vulnerabilidad de gravedad alta durante nuestro último análisis, que aún puede estar expuesta públicamente.

Descripción

Las Vulnerabilidades y exposiciones comunes (en inglés, Common Vulnerabilities and Exposures, siglas CVE) es una lista de vulnerabilidades en software y hardware que son de conocimiento público. Con cada CVE se incluye un ID, una descripción de la vulnerabilidad y los nombres y versiones de los productos afectados por dicha vulnerabilidad.
Los productos de software y hardware suelen informar automáticamente sobre el nombre y la versión de cada producto cuando los hosts se conectan a ellos. Al buscar en la lista de CVE y cruzar esos datos con los nombres y versiones de los productos que se encuentren en la red de la empresa en cuestión, podemos inferir la presencia o ausencia de vulnerabilidades.

Recomendación

Actualice o aplique revisiones al software y al hardware afectados. Habilite las actualizaciones automáticas si están disponibles en su proveedor de software y permitidas en su entorno. Supervise las listas VEC y los repositorios de vulnerabilidades en busca de código de vulnerabilidades que puedan afectar a su infraestructura. Suscríbase a la lista de correo de Bugtraq para recibir alertas sobre nuevas vulnerabilidades a medida que se publiquen. Mantenga una programación de actualización regular para todo el software y hardware en uso dentro de su organización, asegurándose de que se apliquen las últimas revisiones tan pronto como se publiquen.

2 resultados

VULNERABILIDAD	DIRECCIÓN IP	PUERTO	FECHA DE PUBLICACIÓN DE CVE	FECHA DE ÚLTIMA OBSERVACIÓN
CVE-2017-7679	200.53.143.104	443	20/6/2017 0:00:00	14/11/2021 14:12:40
Descripción de vulnerabilidad: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.				
CVE-2017-7679	200.53.143.104	80	20/6/2017 0:00:00	10/11/2021 9:27:14
Descripción de vulnerabilidad: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.				

Patching Cadence (Secuencia de parches) a VEC de gravedad alta

-0.5 IMPACTO EN EL SCORE

High severity vulnerability seen on network more than 45 days after CVE was published.

Descripción

Recomendación

Based on scan data, the company had high severity CVE vulnerability that was open longer than 45 days after the CVE was published. High severity CVEs are those with a documented CVSS severity over 7.0. It is best practice in standards such as PCI DSS to mitigate or patch high severity vulnerabilities within 45 days. Details on each vulnerability are listed in the table below.

Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the National Vulnerability Database (NVD) RSS or other feeds to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.

2 resultados

VULNERABILIDAD	DIRECCIÓN IP	PUERTO	ÚLTIMA OBSERVACIÓN DE APERTURA	FECHA DE PUBLICACIÓN DE VULNERABILIDAD
CVE-2017-7679	200.53.143.104	443	14/11/2021 14:12:40	20/6/2017 0:00:00
Descripción de vulnerabilidad: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.				
CVE-2017-7679	200.53.143.104	80	10/11/2021 9:27:14	20/6/2017 0:00:00
Descripción de vulnerabilidad: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.				

Vulnerabilidad de gravedad media en la última observación

-0.5 IMPACTO EN EL SCORE

Durante nuestro último análisis, hemos observado una vulnerabilidad de gravedad media, que aún puede estar expuesta públicamente.

Descripción

Las Vulnerabilidades y exposiciones comunes (en inglés, Common Vulnerabilities and Exposures, siglas CVE) es una lista de vulnerabilidades en software y hardware que son de conocimiento público. Con cada CVE se incluye un ID, una descripción de la vulnerabilidad y los nombres y versiones de los productos afectados por dicha vulnerabilidad.
Los productos de software y hardware suelen informar automáticamente sobre el nombre y la versión de cada producto cuando los hosts se conectan a ellos. Al buscar en la lista de CVE y cruzar esos datos con los nombres y versiones de los productos que se encuentren en la red de la empresa en cuestión, podemos inferir la presencia o ausencia de vulnerabilidades.

Recomendación

Actualice o aplique revisiones al software y al hardware afectados. Habilite las actualizaciones automáticas si están disponibles en su proveedor de software y permitidas en su entorno. Supervise las listas VEC y los repositorios de vulnerabilidades en busca de código de vulnerabilidades que puedan afectar a su infraestructura. Suscríbase a la lista de correo de Bugtraq para recibir alertas sobre nuevas vulnerabilidades a medida que se publiquen. Mantenga una programación de actualización regular para todo el software y hardware en uso dentro de su organización, asegurándose de que se apliquen las últimas revisiones tan pronto como se publiquen.

28 resultados

VULNERABILIDAD	DIRECCIÓN IP	PUERTO	FECHA DE PUBLICACIÓN DE CVE	FECHA DE ÚLTIMA OBSERVACIÓN
CVE-2017-9798	200.53.143.104	443	18/9/2017 0:00:00	14/11/2021 14:12:40
Descripción de vulnerabilidad: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.				
CVE-2015-3185	200.53.143.104	443	20/7/2015 0:00:00	14/11/2021 14:12:40
Descripción de vulnerabilidad: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2018-1301	200.53.143.104	443	26/3/2018 0:00:00	14/11/2021 14:12:40
Descripción de vulnerabilidad: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.				
CVE-2014-0231	200.53.143.104	443	20/7/2014 0:00:00	14/11/2021 14:12:40
Descripción de vulnerabilidad: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.				
CVE-2014-0098	200.53.143.104	443	18/3/2014 0:00:00	14/11/2021 14:12:40
Descripción de vulnerabilidad: The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.				
CVE-2016-4975	200.53.143.104	443	14/8/2018 0:00:00	14/11/2021 14:12:40

VULNERABILIDAD	DIRECCIÓN IP	PUERTO	FECHA DE PUBLICACIÓN DE CVE	FECHA DE ÚLTIMA OBSERVACIÓN
Descripción de vulnerabilidad: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).				
CVE-2016-8743	200.53.143.104	443	27/7/2017 0:00:00	14/11/2021 14:12:40
Descripción de vulnerabilidad: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.				
CVE-2016-5387	200.53.143.104	443	19/7/2016 0:00:00	14/11/2021 14:12:40
Descripción de vulnerabilidad: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.				
CVE-2017-15715	200.53.143.104	443	26/3/2018 0:00:00	14/11/2021 14:12:40
Descripción de vulnerabilidad: In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.				
CVE-2018-1302	200.53.143.104	443	26/3/2018 0:00:00	14/11/2021 14:12:40
Descripción de vulnerabilidad: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.				
CVE-2018-1312	200.53.143.104	443	26/3/2018 0:00:00	14/11/2021 14:12:40
Descripción de vulnerabilidad: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.				
CVE-2019-0220	200.53.143.104	443	11/6/2019 0:00:00	14/11/2021 14:12:40
Descripción de vulnerabilidad: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.				
CVE-2014-0226	200.53.143.104	443	20/7/2014 0:00:00	14/11/2021 14:12:40
Descripción de vulnerabilidad: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3183	200.53.143.104	443	20/7/2015 0:00:00	14/11/2021 14:12:40
Descripción de vulnerabilidad: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-0231	200.53.143.104	80	20/7/2014 0:00:00	10/11/2021 9:27:14
Descripción de vulnerabilidad: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.				
CVE-2014-0098	200.53.143.104	80	18/3/2014 0:00:00	10/11/2021 9:27:14
Descripción de vulnerabilidad: The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.				
CVE-2018-1301	200.53.143.104	80	26/3/2018 0:00:00	10/11/2021 9:27:14
Descripción de vulnerabilidad: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.				
CVE-2019-0220	200.53.143.104	80	11/6/2019 0:00:00	10/11/2021 9:27:14
Descripción de vulnerabilidad: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.				
CVE-2016-5387	200.53.143.104	80	19/7/2016 0:00:00	10/11/2021 9:27:14
Descripción de vulnerabilidad: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.				
CVE-2015-3185	200.53.143.104	80	20/7/2015 0:00:00	10/11/2021 9:27:14
Descripción de vulnerabilidad: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2016-4975	200.53.143.104	80	14/8/2018 0:00:00	10/11/2021 9:27:14
Descripción de vulnerabilidad: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).				
CVE-2017-9798	200.53.143.104	80	18/9/2017 0:00:00	10/11/2021 9:27:14
Descripción de vulnerabilidad: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.				
CVE-2018-1302	200.53.143.104	80	26/3/2018 0:00:00	10/11/2021 9:27:14
Descripción de vulnerabilidad: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.				

VULNERABILIDAD	DIRECCIÓN IP	PUERTO	FECHA DE PUBLICACIÓN DE CVE	FECHA DE ÚLTIMA OBSERVACIÓN
CVE-2016-8743	200.53.143.104	80	27/7/2017 0:00:00	10/11/2021 9:27:14
Descripción de vulnerabilidad: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.				
CVE-2017-15715	200.53.143.104	80	26/3/2018 0:00:00	10/11/2021 9:27:14
Descripción de vulnerabilidad: In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.				
CVE-2018-1312	200.53.143.104	80	26/3/2018 0:00:00	10/11/2021 9:27:14
Descripción de vulnerabilidad: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.				
CVE-2014-0226	200.53.143.104	80	20/7/2014 0:00:00	10/11/2021 9:27:14
Descripción de vulnerabilidad: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3183	200.53.143.104	80	20/7/2015 0:00:00	10/11/2021 9:27:14
Descripción de vulnerabilidad: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				

Patching Cadence (Secuencia de parches) a VEC de gravedad media

-0.5 IMPACTO EN EL SCORE

Medium severity vulnerability seen on network more than 90 days after CVE was published.

Descripción
Based on scan data, the company had medium severity CVE vulnerability that was open longer than 90 days after the CVE was published. Medium severity CVEs are those with a documented CVSS severity between 4.0 and 6.9. It is best practice to mitigate or patch medium severity vulnerabilities within 90 days. Details on each vulnerability are listed in the table below.

Recomendación
Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the National Vulnerability Database (NVD) RSS or other feeds to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.

28 resultados

VULNERABILIDAD	DIRECCIÓN IP	PUERTO	ÚLTIMA OBSERVACIÓN DE APERTURA	FECHA DE PUBLICACIÓN DE VULNERABILIDAD
CVE-2018-1312	200.53.143.104	443	14/11/2021 14:12:40	26/3/2018 0:00:00
Descripción de vulnerabilidad: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.				
CVE-2014-0231	200.53.143.104	443	14/11/2021 14:12:40	20/7/2014 0:00:00
Descripción de vulnerabilidad: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.				
CVE-2019-0220	200.53.143.104	443	14/11/2021 14:12:40	11/6/2019 0:00:00
Descripción de vulnerabilidad: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.				
CVE-2014-0098	200.53.143.104	443	14/11/2021 14:12:40	18/3/2014 0:00:00
Descripción de vulnerabilidad: The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.				
CVE-2017-9798	200.53.143.104	443	14/11/2021 14:12:40	18/9/2017 0:00:00
Descripción de vulnerabilidad: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.				
CVE-2018-1301	200.53.143.104	443	14/11/2021 14:12:40	26/3/2018 0:00:00
Descripción de vulnerabilidad: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.				
CVE-2016-5387	200.53.143.104	443	14/11/2021 14:12:40	19/7/2016 0:00:00

VULNERABILIDAD	DIRECCIÓN IP	PUERTO	ÚLTIMA OBSERVACIÓN DE APERTURA	FECHA DE PUBLICACIÓN DE VULNERABILIDAD
Descripción de vulnerabilidad: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.				
CVE-2015-3183	200.53.143.104	443	14/11/2021 14:12:40	20/7/2015 0:00:00
Descripción de vulnerabilidad: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-0226	200.53.143.104	443	14/11/2021 14:12:40	20/7/2014 0:00:00
Descripción de vulnerabilidad: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3185	200.53.143.104	443	14/11/2021 14:12:40	20/7/2015 0:00:00
Descripción de vulnerabilidad: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-15715	200.53.143.104	443	14/11/2021 14:12:40	26/3/2018 0:00:00
Descripción de vulnerabilidad: In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.				
CVE-2016-8743	200.53.143.104	443	14/11/2021 14:12:40	27/7/2017 0:00:00
Descripción de vulnerabilidad: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.				
CVE-2018-1302	200.53.143.104	443	14/11/2021 14:12:40	26/3/2018 0:00:00
Descripción de vulnerabilidad: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.				
CVE-2016-4975	200.53.143.104	443	14/11/2021 14:12:40	14/8/2018 0:00:00
Descripción de vulnerabilidad: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).				
CVE-2016-8743	200.53.143.104	80	10/11/2021 9:27:14	27/7/2017 0:00:00
Descripción de vulnerabilidad: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.				
CVE-2016-5387	200.53.143.104	80	10/11/2021 9:27:14	19/7/2016 0:00:00
Descripción de vulnerabilidad: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.				
CVE-2014-0231	200.53.143.104	80	10/11/2021 9:27:14	20/7/2014 0:00:00
Descripción de vulnerabilidad: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.				
CVE-2018-1302	200.53.143.104	80	10/11/2021 9:27:14	26/3/2018 0:00:00
Descripción de vulnerabilidad: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.				
CVE-2018-1312	200.53.143.104	80	10/11/2021 9:27:14	26/3/2018 0:00:00
Descripción de vulnerabilidad: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.				
CVE-2019-0220	200.53.143.104	80	10/11/2021 9:27:14	11/6/2019 0:00:00
Descripción de vulnerabilidad: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.				
CVE-2014-0098	200.53.143.104	80	10/11/2021 9:27:14	18/3/2014 0:00:00
Descripción de vulnerabilidad: The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.				
CVE-2015-3185	200.53.143.104	80	10/11/2021 9:27:14	20/7/2015 0:00:00
Descripción de vulnerabilidad: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	200.53.143.104	80	10/11/2021 9:27:14	20/7/2014 0:00:00
Descripción de vulnerabilidad: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-9798	200.53.143.104	80	10/11/2021 9:27:14	18/9/2017 0:00:00
Descripción de vulnerabilidad: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.				

VULNERABILIDAD	DIRECCIÓN IP	PUERTO	ÚLTIMA OBSERVACIÓN DE APERTURA	FECHA DE PUBLICACIÓN DE VULNERABILIDAD
CVE-2016-4975	200.53.143.104	80	10/11/2021 9:27:14	14/8/2018 0:00:00
Descripción de vulnerabilidad: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).				
CVE-2017-15715	200.53.143.104	80	10/11/2021 9:27:14	26/3/2018 0:00:00
Descripción de vulnerabilidad: In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.				
CVE-2015-3183	200.53.143.104	80	10/11/2021 9:27:14	20/7/2015 0:00:00
Descripción de vulnerabilidad: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2018-1301	200.53.143.104	80	10/11/2021 9:27:14	26/3/2018 0:00:00
Descripción de vulnerabilidad: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.				

A 100 INGENIERÍA SOCIAL

El módulo Social Engineering (Ingeniería Social) de SecurityScorecard se utiliza para determinar la susceptibilidad potencial de una organización a un ataque de ingeniería social dirigido. El módulo Social Engineering ingiere datos de redes sociales y filtraciones de datos públicos, y combina métodos de análisis patentados. La puntuación de Social Engineering es un indicador informativo calculado en función de la cantidad de indicadores que aparecen en los sensores de recolección de SecurityScorecard.

GRAVEDAD ALTA

No hay Problemas de gravedad alta para Social Engineering

GRAVEDAD MEDIA

No hay Problemas de gravedad media para Social Engineering

GRAVEDAD BAJA

No hay Problemas de gravedad baja para Social Engineering

POSITIVA

No hay Señales positivos para Social Engineering

INFORMATIVOS

Exposed Personal Information (Historical)	1

Exposed Personal Information (Historical)

Personal information for individuals associated with employee emails were exposed.

Descripción

Social engineering attacks are significantly more effective when they are used in combination with exposed personal information. For example, security questions to reset account passwords, or to recover accounts that require personal information. Additionally, it's easier for hackers to impersonate employees to gain higher level access. Please note that SecurityScorecard only sees the categories of information associated with exposure.
For privacy reasons, affected user names are only visible to the Administrator of the respective account and are not displayed for other scorecards than you follow.

Recomendación

It's not feasible to remove the information off the internet once exposed so mitigation against social engineering attacks are recommended. Ensure that:
* employees have regular cyber security awareness training * protocols are established for handling sensitive information * periodic, unannounced, tests are performed.

1 resultado

DOMINIO	NOMBRE DE LA FILTRACIÓN	AÑO DE LA FILTRACIÓN	DESCRIPCIÓN	USUARIOS AFECTADOS	FECHA DE ÚLTIMA OBSERVACIÓN
formiik.com	Adapt.io	2018	Adapt.io is a website that provide a business contact database. https://blog.hacken.io/how-sensitive-is-your-non-sensitive-data	beatrizarogelio.barajas	19/11/2018 0:00:00

Ningún contenido (incluidos datos, calificaciones, informes, software u otra aplicación o resultado de los mismos) ya sea en todo o en parte (en su conjunto, el Contenido) puede modificarse, someterse a ingeniería inversa, reproducirse o distribuirse de ninguna forma ni por ningún medio, ni almacenarse en una base de datos o sistema de recuperación, sin el permiso previo por escrito de SecurityScorecard, Inc. (SSC). El Contenido no se utilizará para ningún propósito ilegal o no autorizado.

Ni SSC ni ningún tercero, sus directores, ejecutivos, accionistas, empleados, clientes y agentes (en su conjunto, las Partes de SSC) garantizan la exactitud, integridad, oportunidad o disponibilidad del Contenido. Las Partes de SSC no son responsables de ningún error u omisión (negligente o de otro tipo), independientemente de la causa, ni de los resultados obtenidos del uso del Contenido. El Contenido se proporciona “tal cual”. LAS PARTES DE SECURITYSCORECARD RENUNCIAN A TODAS Y CADA UNA DE LAS GARANTÍAS EXPRESAS O IMPLÍCITAS, INCLUIDAS, ENTRE OTRAS, (1) GARANTÍAS DE COMERCIABILIDAD O IDONEIDAD PARA UN FIN O USO PARTICULAR, (2) GARANTÍAS DE PRECISIÓN, RESULTADOS, OPORTUNIDAD E INTEGRIDAD, (3) GARANTÍAS DE AUSENCIA DE ERRORES O DEFECTOS DE SOFTWARE (4) GARANTÍAS DE FUNCIONAMIENTO ININTERRUMPIDO DEL CONTENIDO Y (5) GARANTÍAS DE FUNCIONAMIENTO DEL CONTENIDO CON CUALQUIER CONFIGURACIÓN DE SOFTWARE O HARDWARE. En ningún caso las Partes de SSC serán responsables ante ninguna de las partes por ningún daño directo, indirecto, incidental, ejemplar, compensatorio, punitivo, especial o consecuente, ni de los costes, gastos, honorarios legales o pérdidas (incluidos, sin limitación, pérdida de beneficios o lucro cesante y costes o pérdidas de oportunidad causados por negligencia) en relación con cualquier uso del Contenido, incluso si se les informa de la posibilidad de tales daños.

LOS USUARIOS DEL CONTENIDO DEBEN HACER TODOS LOS ESFUERZOS RAZONABLES PARA MITIGAR CUALQUIER PÉRDIDA O DAÑO DE CUALQUIER TIPO (Y POR CUALQUIER CAUSA) Y NADA DE LO QUE FIGURE EN EL PRESENTE DOCUMENTO SE CONSIDERARÁ QUE EXIME O ANULA EL DEBER DE LOS USUARIOS DE MITIGAR CUALQUIER PÉRDIDA O DAÑO.

EN CUALQUIER CASO, EN LA MEDIDA PERMITIDA POR LA LEY, LA RESPONSABILIDAD AGREGADA DE LAS PARTES DE SSC RELACIONADA POR CUALQUIER RAZÓN CON EL ACCESO O EL USO DEL CONTENIDO NO SUPERARÁ LA CANTIDAD MAYOR ENTRE (A) EL IMPORTE TOTAL QUE EL USUARIO HAYA PAGADO A SSC POR LOS SERVICIOS PRESTADOS DURANTE LOS 12 MESES INMEDIATAMENTE ANTERIORES AL EVENTO QUE DA LUGAR A LA RESPONSABILIDAD, Y (B) 100 USD.

Los análisis relacionados con la seguridad, incluidas las calificaciones, y las declaraciones que figuren en el Contenido son declaraciones de opinión sobre los riesgos de seguridad relativos futuros de las entidades en la fecha en que se expresan, y no declaraciones de hechos actuales o históricos en cuanto a la seguridad de las transacciones con cualquier entidad, ni recomendaciones sobre la decisión de hacer negocios con cualquier entidad, ni avales de la exactitud de cualquiera de los datos o conclusiones o intentos de evaluar o dar fe de forma independiente de las medidas de seguridad de cualquier entidad. Las opiniones, análisis y calificaciones de SSC no deben utilizarse como sustituto de la habilidad, el buen juicio y la experiencia del usuario y de sus directivos, empleados, asesores y clientes a la hora de tomar decisiones empresariales. SSC no asume ninguna obligación de actualizar el Contenido después de su publicación en cualquier forma ni formato. Si bien SSC ha obtenido información de fuentes que considera fiables, no realiza ninguna auditoría y no asume ninguna obligación de diligencia debida ni verificación independiente de ninguna información que recibe. Los Usuarios acuerdan expresamente que (a) las calificaciones de seguridad y otras opiniones de seguridad proporcionadas a través del Contenido no reflejan, identifican ni detectan cada vulnerabilidad o problema de seguridad ni abordan ningún otro riesgo; (b) las calificaciones de seguridad y otras opiniones proporcionadas no tienen en cuenta los objetivos, situaciones o necesidades particulares de los usuarios; (c) cada calificación u otra opinión se ponderará, si corresponde, únicamente como un factor en cualquier decisión tomada por cualquier usuario o en nombre de este; y (d) los usuarios, en consecuencia, con el debido cuidado, realizarán su propio estudio y evaluación de los riesgos de hacer negocios con cualquier entidad. Si un usuario identifica alguno en el Contenido, le invitamos a compartir esa información con nosotros enviándonos un correo electrónico a support@securityscorecard.io.