INFORME DE VULNERABILIDADES
Seguridad Informática

INFORME DE VULNERABILIDADES

Empresa: Empresa ficticia sl

Noviembre 2025

Índice

Resumen Ejecutivo

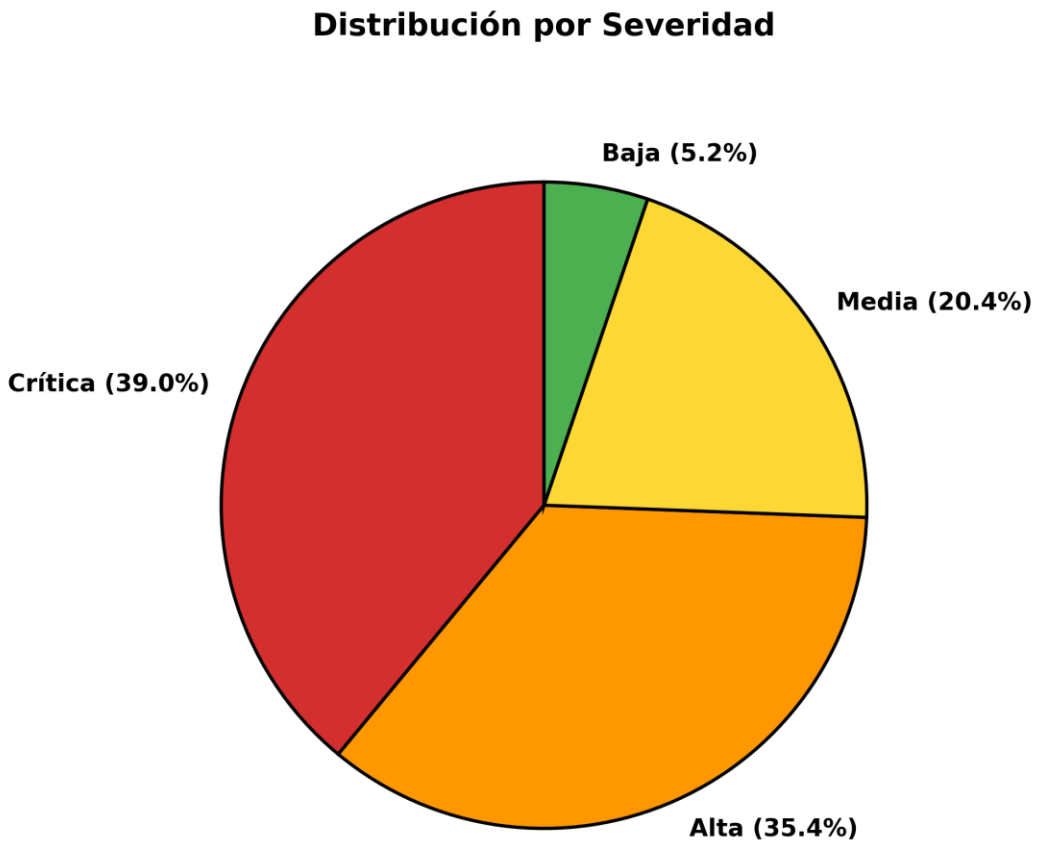
Durante el análisis de Noviembre 2025, se identificaron 1000 vulnerabilidades en 50 hosts. Críticas: 390, Altas: 354.

Métricas Generales

Métrica	Valor
Total	1000
CVEs Únicos	24
Hosts	50
Críticas	390
Altas	354
Medias	204
Bajas	52

Análisis por Severidad

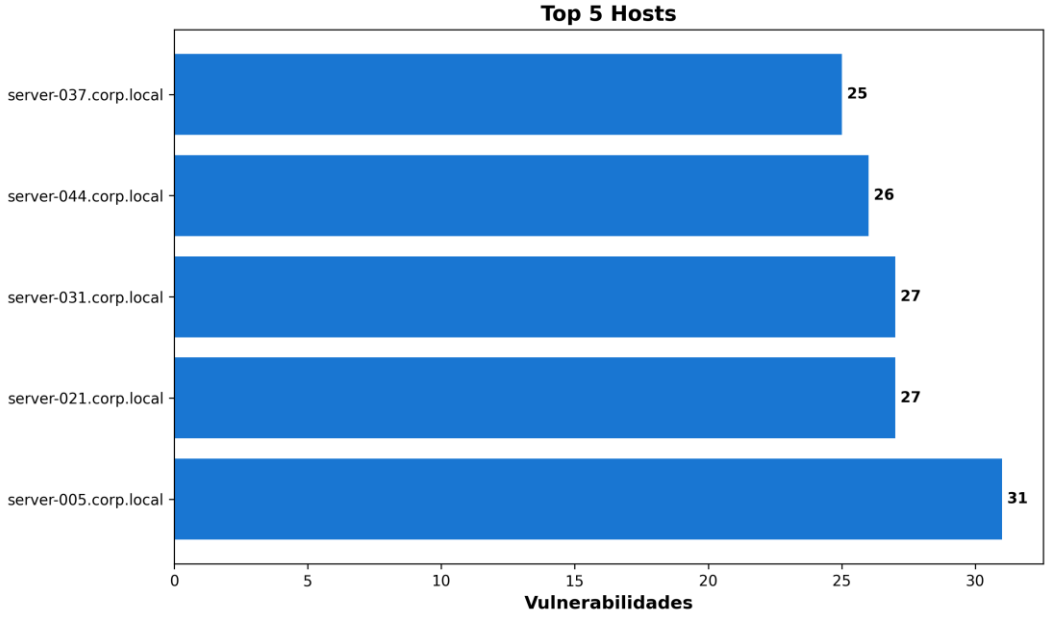
Distribución de vulnerabilidades por nivel de riesgo.



Análisis de Infraestructura

Top 5 Hosts

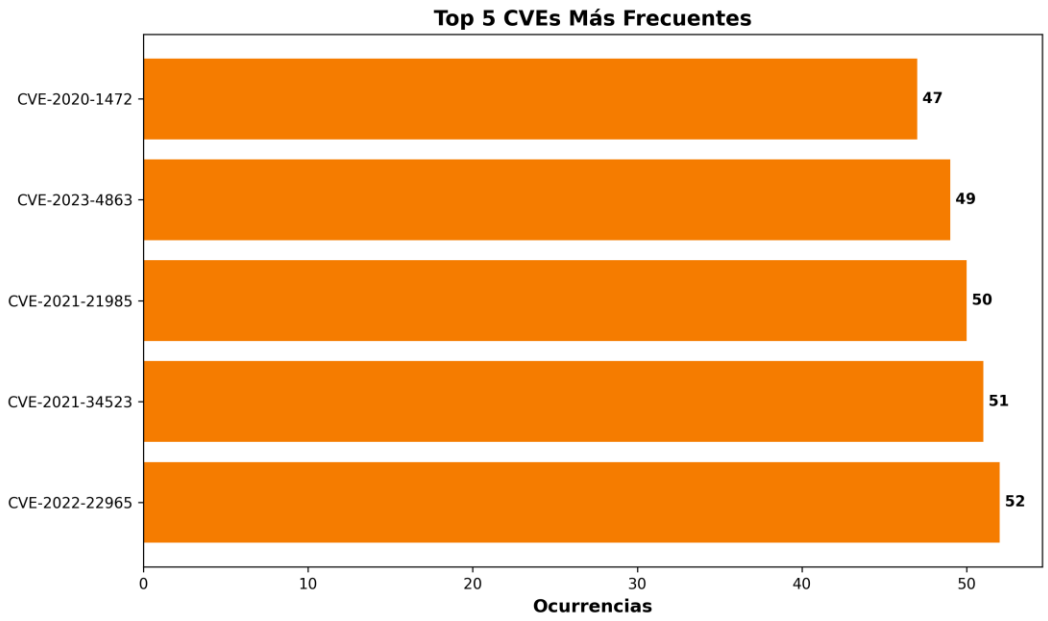
Host	Tot	Crit	Alt	Med	Baj
server-005.corp.local	31	11	8	8	4
server-021.corp.local	27	8	8	10	1
server-031.corp.local	27	9	13	4	1
server-044.corp.local	26	7	12	7	0
server-037.corp.local	25	12	10	2	1



Análisis de CVEs

Top 5 CVEs

CVE	Ocur	Sev	Hosts
CVE-2022-22965	52	Critical	32
CVE-2021-34523	51	Critical	33
CVE-2021-21985	50	Critical	30
CVE-2023-4863	49	Critical	33
CVE-2020-1472	47	Critical	33



Vulnerabilidades Críticas

CVE-2021-34527

Detalle técnico: Una vulnerabilidad en la ejecución de código remota de Windows Print Spooler

Ocurrencias: 18

Hosts afectados: 16

Paquete: print-spooler

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-34527

CVE-2019-19781

Detalle técnico: Se descubrió un problema en Citrix Application Delivery Controller (ADC) and Gateway versiones 10.5, 11.1, 12.0, 12.1 y 13.0. Permiten un salto de directorio.

Ocurrencias: 17

Hosts afectados: 15

Paquete: citrix-adc

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2019-19781

CVE-2021-26857

Detalle técnico: Una Vulnerabilidad de Ejecución de código remota de Microsoft Exchange Server. Este ID de CVE es diferente de CVE-2021-26412, CVE-2021-26854, CVE-2021-26855, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078

Ocurrencias: 18

Hosts afectados: 16

Paquete: exchange-deserializer

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-26857

CVE-2021-44228

Detalle técnico: Las características JNDI de Apache Log4j2 2.0-beta9 hasta 2.15.0 (excluyendo las versiones de seguridad 2.12.2, 2.12.3 y 2.3.1) utilizadas en la configuración, los mensajes de

registro y los parámetros no protegen contra LDAP controlado por un atacante y otros puntos finales relacionados con JNDI. Un atacante que pueda controlar los mensajes de registro o los parámetros de los mensajes de registro puede ejecutar código arbitrario cargado desde servidores LDAP cuando la sustitución de la búsqueda de mensajes está habilitada. A partir de la versión 2.15.0 de log4j, este comportamiento ha sido...

Ocurrencias: 14

Hosts afectados: 13

Paquete: log4j-core

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-44228

CVE-2023-36884

Detalle técnico: Windows Search Remote Code Execution Vulnerability

Ocurrencias: 16

Hosts afectados: 13

Paquete: windows-kernel

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-36884

CVE-2018-11776

Detalle técnico: Apache Struts, desde la versión 2.3 hasta la 2.3.34 y desde la versión 2.5 hasta la 2.5.16, sufre de una posible ejecución remota de código cuando el valor de alwaysSelectFullNamespace es "true" (establecido por el usuario o por un plugin como Convention Plugin). Además, los resultados se emplean sin ningún espacio de nombres y, al mismo tiempo, el paquete superior no tiene espacio de nombres o contiene caracteres comodín. De manera similar a como pasa con los resultados, existe la misma posibilidad al emplear la etiqueta url, que no tiene un valor y acción definidos y, además, su paquete s...

Ocurrencias: 15

Hosts afectados: 14

Paquete: apache-struts

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2018-11776

CVE-2022-1388

Detalle técnico: En F5 BIG-IP versiones 16.1.x anteriores a 16.1.2.2, versiones 15.1.x anteriores a 15.1.5.1, versiones 14.1.x anteriores a 14.1.4.6, versiones 13.1.x anteriores a 13.1.5 y todas las versiones 12.1.x y 11.6.x, las peticiones no reveladas pueden omitir la autenticación REST de iControl. Nota: las versiones de software que han alcanzado el Fin del Soporte Técnico (EoTS) no son evaluadas

Ocurrencias: 14

Hosts afectados: 11

Paquete: f5-bigip

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-1388

CVE-2018-13379

Detalle técnico: Una limitación inadecuada de un nombre de ruta a un directorio restringido ("Path Traversal") en Fortinet FortiOS versiones 6.0.0 a 6.0.4, 5.6.3 a 5.6.7 y 5.4.6 a 5.4.12 y FortiProxy versiones 2.0.0, 1. 2.0 a 1.2.8, 1.1.0 a 1.1.6, 1.0.0 a 1.0.7 bajo el portal web SSL VPN permite a un atacante no autenticado descargar archivos del sistema a través de solicitudes de recursos HTTP especialmente diseñadas

Ocurrencias: 9

Hosts afectados: 9

Paquete: fortinet-vpn

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2018-13379

CVE-2018-8174

Detalle técnico: Existe una vulnerabilidad de ejecución remota de código debido a la forma en la que el motor VBScript gestiona los objetos en la memoria. Esto también se conoce como "Windows VBScript Engine Remote Code Execution Vulnerability". Esto afecta a Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10 y Windows 10 Servers.

Ocurrencias: 18

Hosts afectados: 15

Paquete: vbscript-engine

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2018-8174

CVE-2022-22965

Detalle técnico: Una aplicación Spring MVC o Spring WebFlux que es ejecutada en JDK 9+ puede ser vulnerable a la ejecución de código remota (RCE) por medio de una vinculación de datos. La explotación específica requiere que la aplicación sea ejecutada en Tomcat como un despliegue WAR. Si la aplicación es desplegada como un jar ejecutable de Spring Boot, es decir, por defecto, no es vulnerable a la explotación. Sin embargo, la naturaleza de la vulnerabilidad es más general, y puede haber otras formas de explotarla

Ocurrencias: 20

Hosts afectados: 17

Paquete: spring-framework

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-22965

CVE-2021-26855

Detalle técnico: Una Vulnerabilidad de Ejecución de código remota de Microsoft Exchange Server. Este ID de CVE es diferente de CVE-2021-26412, CVE-2021-26854, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078

Ocurrencias: 21

Hosts afectados: 17

Paquete: exchange-server

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-26855

CVE-2023-41064

Detalle técnico: Se solucionó un problema de Desbordamiento de Búfer de manejo de la memoria mejorada. Este problema se solucionó en macOS Monterey 12.6.9, macOS Big Sur 11.7.10, macOS Ventura 13.5.2, iOS 16.6.1 y iPadOS 16.6.1, iOS 15.7.9 y iPadOS 15.7.9. El procesamiento de una imagen creada con fines maliciosos puede provocar la ejecución de código arbitrario. Apple está al tanto de un informe de que este problema puede haber sido explotado activamente.

Ocurrencias: 13

Hosts afectados: 11

Paquete: imessage

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-41064

CVE-2024-30088

Detalle técnico: Vulnerabilidad de elevación de privilegios del kernel de Windows

Ocurrencias: 14

Hosts afectados: 12

Paquete: tpm-driver

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2024-30088

CVE-2020-0601

Detalle técnico: Se presenta una vulnerabilidad de suplantación de identidad en la manera en que Windows CryptoAPI (Crypt32.dll) comprueba los certificados Elliptic Curve Cryptography (ECC). Un atacante podría explotar la vulnerabilidad mediante el uso de un certificado de firma de código falsificado para firmar un ejecutable malicioso, haciendo que parezca que el archivo era de una fuente confiable y legítima, también se conoce como "Windows CryptoAPI Spoofing Vulnerability".

Ocurrencias: 21

Hosts afectados: 16

Paquete: windows-cryptoapi

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2020-0601

CVE-2023-28432

Detalle técnico: Minio is a Multi-Cloud Object Storage framework. In a cluster deployment starting with RELEASE.2019-12-17T23-16-33Z and prior to RELEASE.2023-03-20T20-16-18Z, MinIO returns all environment variables, including `MINIO_SECRET_KEY` and `MINIO_ROOT_PASSWORD`, resulting in information disclosure. All users of distributed deployment are impacted. All users are advised to upgrade to RELEASE.2023-03-20T20-16-18Z.

Ocurrencias: 16

Hosts afectados: 14

Paquete: office

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-28432

CVE-2021-34523

Detalle técnico: Una vulnerabilidad de Elevación de Privilegios de Microsoft Exchange Server. Este ID de CVE es diferente de CVE-2021-33768, CVE-2021-34470

Ocurrencias: 20

Hosts afectados: 19

Paquete: exchange-elev

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-34523

CVE-2017-0144

Detalle técnico: El servidor SMBv1 en Microsoft Windows Vista SP2; Windows Server 2008 SP2 y R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold y R2; Windows RT 8.1; y Windows 10 Gold, 1511 y 1607; y Windows Server 2016 permite a atacantes remotos ejecutar código arbitrario a través de paquetes manipulados, vulnerabilidad también conocida como "Windows SMB Remote Code Execution Vulnerability". Esta vulnerabilidad es diferente a la descrita en CVE-2017-0143, CVE-2017-0145, CVE-2017-0146 y CVE-2017-0148.

Ocurrencias: 15

Hosts afectados: 13

Paquete: smb-server

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2017-0144

CVE-2021-21985

Detalle técnico: VSphere Client (HTML5) contiene una vulnerabilidad de ejecución de código remota debido a una falta de comprobación de entrada en el plugin Virtual SAN Health Check, que está habilitado por defecto en vCenter Server. Un actor malicioso con acceso de red al

puerto 443 puede explotar este problema para ejecutar comandos con privilegios ilimitados en el sistema operativo subyacente que aloja a vCenter Server

Ocurrencias: 19

Hosts afectados: 16

Paquete: vmware-vcenter

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-21985

CVE-2023-23397

Detalle técnico: Microsoft Outlook Elevation of Privilege Vulnerability

Ocurrencias: 17

Hosts afectados: 15

Paquete: outlook

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-23397

CVE-2024-21338

Detalle técnico: Vulnerabilidad de elevación de privilegios del kernel de Windows

Ocurrencias: 13

Hosts afectados: 11

Paquete: minio

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2024-21338

CVE-2019-0708

Detalle técnico: Existe una vulnerabilidad de ejecución remota de código en Remote Desktop Services, anteriormente conocido como Terminal Services, cuando un atacante no autenticado se conecta al sistema de destino mediante RDP y envía peticiones especialmente diseñadas, conocida como 'Remote Desktop Services Remote Code Execution Vulnerability'.

Ocurrencias: 11

Hosts afectados: 10

Paquete: rdp-service

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2019-0708

CVE-2023-4863

Detalle técnico: El desbordamiento del búfer de memoria en libwebp en Google Chrome anterior a 116.0.5845.187 y libwebp 1.3.2 permitía a un atacante remoto realizar una escritura en memoria fuera de los límites a través de una página HTML manipulada. (Severidad de seguridad de Chromium: crítica)

Ocurrencias: 18

Hosts afectados: 16

Paquete: chrome

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-4863

CVE-2022-3602

Detalle técnico: Puede activarse una saturación del búfer en la verificación del certificado X.509, específicamente en la verificación de restricciones en el nombre. Tenga en cuenta que esto ocurre después de la verificación de la firma de la cadena de certificados y requiere que una CA haya firmado el certificado malicioso o que la aplicación continúe con la verificación del certificado a pesar de no poder construir una ruta a un emisor confiable. Un atacante puede crear una dirección de correo electrónico maliciosa para desbordar cuatro bytes en la pila de memoria controlados por el atacante. Este desbord...

Ocurrencias: 18

Hosts afectados: 17

Paquete: openssl

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-3602

CVE-2020-1472

Detalle técnico: Se presenta una vulnerabilidad de elevación de privilegios cuando un atacante establece una conexión de canal seguro Netlogon vulnerable hacia un controlador de dominio, usando el Netlogon Remote Protocol (MS-NRPC), también se conoce como "Netlogon Elevation of Privilege Vulnerability".

Ocurrencias: 15

Hosts afectados: 15

Paquete: netlogon

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2020-1472

Vulnerabilidades Altas

CVE-2023-36884

Detalle técnico: Windows Search Remote Code Execution Vulnerability

Ocurrencias: 18

Hosts afectados: 17

Paquete: windows-kernel

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-36884

CVE-2022-3602

Detalle técnico: Puede activarse una saturación del búfer en la verificación del certificado X.509, específicamente en la verificación de restricciones en el nombre. Tenga en cuenta que esto ocurre después de la verificación de la firma de la cadena de certificados y requiere que una CA haya firmado el certificado malicioso o que la aplicación continúe con la verificación del certificado a pesar de no poder construir una ruta a un emisor confiable. Un atacante puede crear una dirección de correo electrónico maliciosa para desbordar cuatro bytes en la pila de memoria controlados por el atacante. Este desbord...

Ocurrencias: 17

Hosts afectados: 15

Paquete: openssl

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-3602

CVE-2023-28432

Detalle técnico: Minio is a Multi-Cloud Object Storage framework. In a cluster deployment starting with RELEASE.2019-12-17T23-16-33Z and prior to RELEASE.2023-03-20T20-16-18Z, MinIO returns all environment variables, including `MINIO_SECRET_KEY` and `MINIO_ROOT_PASSWORD`, resulting in information disclosure. All users of distributed deployment are impacted. All users are advised to upgrade to RELEASE.2023-03-20T20-16-18Z.

Ocurrencias: 8

Hosts afectados: 8

Paquete: office

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-28432

CVE-2018-8174

Detalle técnico: Existe una vulnerabilidad de ejecución remota de código debido a la forma en la que el motor VBScript gestiona los objetos en la memoria. Esto también se conoce como "Windows VBScript Engine Remote Code Execution Vulnerability". Esto afecta a Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10 y Windows 10 Servers.

Ocurrencias: 14

Hosts afectados: 14

Paquete: vbscript-engine

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2018-8174

CVE-2023-4863

Detalle técnico: El desbordamiento del búfer de memoria en libwebp en Google Chrome anterior a 116.0.5845.187 y libwebp 1.3.2 permitía a un atacante remoto realizar una escritura en memoria fuera de los límites a través de una página HTML manipulada. (Severidad de seguridad de Chromium: crítica)

Ocurrencias: 15

Hosts afectados: 12

Paquete: chrome

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-4863

CVE-2019-0708

Detalle técnico: Existe una vulnerabilidad de ejecución remota de código en Remote Desktop Services, anteriormente conocido como Terminal Services, cuando un atacante no autenticado se conecta al sistema de destino mediante RDP y envía peticiones especialmente diseñadas, conocida como 'Remote Desktop Services Remote Code Execution Vulnerability'.

Ocurrencias: 14

Hosts afectados: 12

Paquete: rdp-service

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2019-0708

CVE-2020-1472

Detalle técnico: Se presenta una vulnerabilidad de elevación de privilegios cuando un atacante establece una conexión de canal seguro Netlogon vulnerable hacia un controlador de dominio, usando el Netlogon Remote Protocol (MS-NRPC), también se conoce como "Netlogon Elevation of Privilege Vulnerability".

Ocurrencias: 15

Hosts afectados: 12

Paquete: netlogon

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2020-1472

CVE-2021-26857

Detalle técnico: Una Vulnerabilidad de Ejecución de código remota de Microsoft Exchange Server. Este ID de CVE es diferente de CVE-2021-26412, CVE-2021-26854, CVE-2021-26855, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078

Ocurrencias: 14

Hosts afectados: 9

Paquete: exchange-deserializer

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-26857

CVE-2024-30088

Detalle técnico: Vulnerabilidad de elevación de privilegios del kernel de Windows

Ocurrencias: 19

Hosts afectados: 16

Paquete: tpm-driver

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2024-30088

CVE-2024-21338

Detalle técnico: Vulnerabilidad de elevación de privilegios del kernel de Windows

Ocurrencias: 20

Hosts afectados: 14

Paquete: minio

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2024-21338

CVE-2018-13379

Detalle técnico: Una limitación inadecuada de un nombre de ruta a un directorio restringido ("Path Traversal") en Fortinet FortiOS versiones 6.0.0 a 6.0.4, 5.6.3 a 5.6.7 y 5.4.6 a 5.4.12 y FortiProxy versiones 2.0.0, 1. 2.0 a 1.2.8, 1.1.0 a 1.1.6, 1.0.0 a 1.0.7 bajo el portal web SSL VPN permite a un atacante no autenticado descargar archivos del sistema a través de solicitudes de recursos HTTP especialmente diseñadas

Ocurrencias: 11

Hosts afectados: 11

Paquete: fortinet-vpn

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2018-13379

CVE-2021-34527

Detalle técnico: Una vulnerabilidad en la ejecución de código remota de Windows Print Spooler

Ocurrencias: 14

Hosts afectados: 12

Paquete: print-spooler

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-34527

CVE-2021-21985

Detalle técnico: VSphere Client (HTML5) contiene una vulnerabilidad de ejecución de código remota debido a una falta de comprobación de entrada en el plugin Virtual SAN Health Check, que está habilitado por defecto en vCenter Server. Un actor malicioso con acceso de red al puerto 443 puede explotar este problema para ejecutar comandos con privilegios ilimitados en el sistema operativo subyacente que aloja a vCenter Server

Ocurrencias: 18

Hosts afectados: 15

Paquete: vmware-vcenter

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-21985

CVE-2021-26855

Detalle técnico: Una Vulnerabilidad de Ejecución de código remota de Microsoft Exchange Server. Este ID de CVE es diferente de CVE-2021-26412, CVE-2021-26854, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078

Ocurrencias: 14

Hosts afectados: 13

Paquete: exchange-server

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-26855

CVE-2021-34523

Detalle técnico: Una vulnerabilidad de Elevación de Privilegios de Microsoft Exchange Server. Este ID de CVE es diferente de CVE-2021-33768, CVE-2021-34470

Ocurrencias: 20

Hosts afectados: 17

Paquete: exchange-elev

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-34523

CVE-2022-22965

Detalle técnico: Una aplicación Spring MVC o Spring WebFlux que es ejecutada en JDK 9+ puede ser vulnerable a la ejecución de código remota (RCE) por medio de una vinculación de datos. La explotación específica requiere que la aplicación sea ejecutada en Tomcat como un despliegue WAR. Si la aplicación es desplegada como un jar ejecutable de Spring Boot, es decir, por defecto, no es vulnerable a la explotación. Sin embargo, la naturaleza de la vulnerabilidad es más general, y puede haber otras formas de explotarla

Ocurrencias: 15

Hosts afectados: 11

Paquete: spring-framework

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-22965

CVE-2019-19781

Detalle técnico: Se descubrió un problema en Citrix Application Delivery Controller (ADC) and Gateway versiones 10.5, 11.1, 12.0, 12.1 y 13.0. Permiten un salto de directorio.

Ocurrencias: 17

Hosts afectados: 14

Paquete: citrix-adc

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2019-19781

CVE-2022-1388

Detalle técnico: En F5 BIG-IP versiones 16.1.x anteriores a 16.1.2.2, versiones 15.1.x anteriores a 15.1.5.1, versiones 14.1.x anteriores a 14.1.4.6, versiones 13.1.x anteriores a 13.1.5 y todas las versiones 12.1.x y 11.6.x, las peticiones no reveladas pueden omitir la autenticación REST de iControl. Nota: las versiones de software que han alcanzado el Fin del Soporte Técnico (EoTS) no son evaluadas

Ocurrencias: 17

Hosts afectados: 14

Paquete: f5-bigip

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-1388

CVE-2021-44228

Detalle técnico: Las características JNDI de Apache Log4j2 2.0-beta9 hasta 2.15.0 (excluyendo las versiones de seguridad 2.12.2, 2.12.3 y 2.3.1) utilizadas en la configuración, los mensajes de registro y los parámetros no protegen contra LDAP controlado por un atacante y otros puntos finales relacionados con JNDI. Un atacante que pueda controlar los mensajes de registro o los parámetros de los mensajes de registro puede ejecutar código arbitrario cargado desde servidores LDAP cuando la sustitución de la búsqueda de mensajes está habilitada. A partir de la versión 2.15.0 de log4j, este comportamiento ha sido...

Ocurrencias: 14

Hosts afectados: 12

Paquete: log4j-core

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-44228

CVE-2020-0601

Detalle técnico: Se presenta una vulnerabilidad de suplantación de identidad en la manera en que Windows CryptoAPI (Crypt32.dll) comprueba los certificados Elliptic Curve Cryptography (ECC). Un atacante podría explotar la vulnerabilidad mediante el uso de un certificado de firma de código falsificado para firmar un ejecutable malicioso, haciendo que parezca que el archivo era de una fuente confiable y legítima, también se conoce como "Windows CryptoAPI Spoofing Vulnerability".

Ocurrencias: 9

Hosts afectados: 8

Paquete: windows-cryptoapi

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2020-0601

CVE-2017-0144

Detalle técnico: El servidor SMBv1 en Microsoft Windows Vista SP2; Windows Server 2008 SP2 y R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold y R2; Windows RT 8.1; y Windows 10 Gold, 1511 y 1607; y Windows Server 2016 permite a atacantes remotos ejecutar código arbitrario a través de paquetes manipulados, vulnerabilidad también conocida como "Windows SMB Remote Code Execution Vulnerability". Esta vulnerabilidad es diferente a la descrita en CVE-2017-0143, CVE-2017-0145, CVE-2017-0146 y CVE-2017-0148.

Ocurrencias: 14

Hosts afectados: 12

Paquete: smb-server

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2017-0144

CVE-2023-41064

Detalle técnico: Se solucionó un problema de Desbordamiento de Búfer de manejo de la memoria mejorada. Este problema se solucionó en macOS Monterey 12.6.9, macOS Big Sur 11.7.10, macOS Ventura 13.5.2, iOS 16.6.1 y iPadOS 16.6.1, iOS 15.7.9 y iPadOS 15.7.9. El procesamiento de una imagen creada con fines maliciosos puede provocar la ejecución de código arbitrario. Apple está al tanto de un informe de que este problema puede haber sido explotado activamente.

Ocurrencias: 16

Hosts afectados: 15

Paquete: imessage

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-41064

CVE-2018-11776

Detalle técnico: Apache Struts, desde la versión 2.3 hasta la 2.3.34 y desde la versión 2.5 hasta la 2.5.16, sufre de una posible ejecución remota de código cuando el valor de alwaysSelectFullNamespace es "true" (establecido por el usuario o por un plugin como Convention Plugin). Además, los resultados se emplean sin ningún espacio de nombres y, al mismo tiempo, el paquete superior no tiene espacio de nombres o contiene caracteres comodín. De manera similar a como pasa con los resultados, existe la misma posibilidad al emplear la etiqueta url, que no tiene un valor y acción definidos y, además, su paquete s...

Ocurrencias: 12

Hosts afectados: 9

Paquete: apache-struts

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2018-11776

CVE-2023-23397

Detalle técnico: Microsoft Outlook Elevation of Privilege Vulnerability

Ocurrencias: 9

Hosts afectados: 9

Paquete: outlook

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-23397

Vulnerabilidades Medias

CVE-2023-4863

Detalle técnico: El desbordamiento del búfer de memoria en libwebp en Google Chrome anterior a 116.0.5845.187 y libwebp 1.3.2 permitía a un atacante remoto realizar una escritura en memoria fuera de los límites a través de una página HTML manipulada. (Severidad de seguridad de Chromium: crítica)

Ocurrencias: 15

Hosts afectados: 15

Paquete: chrome

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-4863

CVE-2021-21985

Detalle técnico: VSphere Client (HTML5) contiene una vulnerabilidad de ejecución de código remota debido a una falta de comprobación de entrada en el plugin Virtual SAN Health Check, que está habilitado por defecto en vCenter Server. Un actor malicioso con acceso de red al puerto 443 puede explotar este problema para ejecutar comandos con privilegios ilimitados en el sistema operativo subyacente que aloja a vCenter Server

Ocurrencias: 9

Hosts afectados: 9

Paquete: vmware-vcenter

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-21985

CVE-2023-41064

Detalle técnico: Se solucionó un problema de Desbordamiento de Búfer de manejo de la memoria mejorada. Este problema se solucionó en macOS Monterey 12.6.9, macOS Big Sur 11.7.10, macOS Ventura 13.5.2, iOS 16.6.1 y iPadOS 16.6.1, iOS 15.7.9 y iPadOS 15.7.9. El procesamiento de una imagen creada con fines maliciosos puede provocar la ejecución de código arbitrario. Apple está al tanto de un informe de que este problema puede haber sido explotado activamente.

Ocurrencias: 5

Hosts afectados: 5

Paquete: imessage

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-41064

CVE-2021-26857

Detalle técnico: Una Vulnerabilidad de Ejecución de código remota de Microsoft Exchange Server. Este ID de CVE es diferente de CVE-2021-26412, CVE-2021-26854, CVE-2021-26855, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078

Ocurrencias: 8

Hosts afectados: 8

Paquete: exchange-deserializer

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-26857

CVE-2024-21338

Detalle técnico: Vulnerabilidad de elevación de privilegios del kernel de Windows

Ocurrencias: 11

Hosts afectados: 9

Paquete: minio

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2024-21338

CVE-2021-34527

Detalle técnico: Una vulnerabilidad en la ejecución de código remota de Windows Print Spooler

Ocurrencias: 6

Hosts afectados: 6

Paquete: print-spooler

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-34527

CVE-2022-1388

Detalle técnico: En F5 BIG-IP versiones 16.1.x anteriores a 16.1.2.2, versiones 15.1.x anteriores a 15.1.5.1, versiones 14.1.x anteriores a 14.1.4.6, versiones 13.1.x anteriores a 13.1.5 y todas las versiones 12.1.x y 11.6.x, las peticiones no reveladas pueden omitir la autenticación REST de iControl. Nota: las versiones de software que han alcanzado el Fin del Soporte Técnico (EoTS) no son evaluadas

Ocurrencias: 8

Hosts afectados: 8

Paquete: f5-bigip

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-1388

CVE-2022-22965

Detalle técnico: Una aplicación Spring MVC o Spring WebFlux que es ejecutada en JDK 9+ puede ser vulnerable a la ejecución de código remota (RCE) por medio de una vinculación de datos. La explotación específica requiere que la aplicación sea ejecutada en Tomcat como un despliegue WAR. Si la aplicación es desplegada como un jar ejecutable de Spring Boot, es decir, por defecto, no es vulnerable a la explotación. Sin embargo, la naturaleza de la vulnerabilidad es más general, y puede haber otras formas de explotarla

Ocurrencias: 15

Hosts afectados: 13

Paquete: spring-framework

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-22965

CVE-2020-0601

Detalle técnico: Se presenta una vulnerabilidad de suplantación de identidad en la manera en que Windows CryptoAPI (Crypt32.dll) comprueba los certificados Elliptic Curve Cryptography (ECC). Un atacante podría explotar la vulnerabilidad mediante el uso de un certificado de firma de código falsificado para firmar un ejecutable malicioso, haciendo que parezca que el archivo era de una fuente confiable y legítima, también se conoce como "Windows CryptoAPI Spoofing Vulnerability".

Ocurrencias: 10

Hosts afectados: 10

Paquete: windows-cryptoapi

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2020-0601

CVE-2020-1472

Detalle técnico: Se presenta una vulnerabilidad de elevación de privilegios cuando un atacante establece una conexión de canal seguro Netlogon vulnerable hacia un controlador de dominio, usando el Netlogon Remote Protocol (MS-NRPC), también se conoce como "Netlogon Elevation of Privilege Vulnerability".

Ocurrencias: 14

Hosts afectados: 13

Paquete: netlogon

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2020-1472

CVE-2018-13379

Detalle técnico: Una limitación inadecuada de un nombre de ruta a un directorio restringido ("Path Traversal") en Fortinet FortiOS versiones 6.0.0 a 6.0.4, 5.6.3 a 5.6.7 y 5.4.6 a 5.4.12 y FortiProxy versiones 2.0.0, 1. 2.0 a 1.2.8, 1.1.0 a 1.1.6, 1.0.0 a 1.0.7 bajo el portal web SSL VPN permite a un atacante no autenticado descargar archivos del sistema a través de solicitudes de recursos HTTP especialmente diseñadas

Ocurrencias: 7

Hosts afectados: 7

Paquete: fortinet-vpn

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2018-13379

CVE-2021-34523

Detalle técnico: Una vulnerabilidad de Elevación de Privilegios de Microsoft Exchange Server. Este ID de CVE es diferente de CVE-2021-33768, CVE-2021-34470

Ocurrencias: 9

Hosts afectados: 9

Paquete: exchange-elev

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-34523

CVE-2024-30088

Detalle técnico: Vulnerabilidad de elevación de privilegios del kernel de Windows

Ocurrencias: 7

Hosts afectados: 7

Paquete: tpm-driver

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2024-30088

CVE-2019-19781

Detalle técnico: Se descubrió un problema en Citrix Application Delivery Controller (ADC) and Gateway versiones 10.5, 11.1, 12.0, 12.1 y 13.0. Permiten un salto de directorio.

Ocurrencias: 7

Hosts afectados: 7

Paquete: citrix-adc

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2019-19781

CVE-2021-26855

Detalle técnico: Una Vulnerabilidad de Ejecución de código remota de Microsoft Exchange Server. Este ID de CVE es diferente de CVE-2021-26412, CVE-2021-26854, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078

Ocurrencias: 10

Hosts afectados: 8

Paquete: exchange-server

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-26855

CVE-2023-36884

Detalle técnico: Windows Search Remote Code Execution Vulnerability

Ocurrencias: 8

Hosts afectados: 8

Paquete: windows-kernel

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-36884

CVE-2019-0708

Detalle técnico: Existe una vulnerabilidad de ejecución remota de código en Remote Desktop Services, anteriormente conocido como Terminal Services, cuando un atacante no autenticado se conecta al sistema de destino mediante RDP y envía peticiones especialmente diseñadas, conocida como 'Remote Desktop Services Remote Code Execution Vulnerability'.

Ocurrencias: 9

Hosts afectados: 8

Paquete: rdp-service

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2019-0708

CVE-2018-8174

Detalle técnico: Existe una vulnerabilidad de ejecución remota de código debido a la forma en la que el motor VBScript gestiona los objetos en la memoria. Esto también se conoce como "Windows VBScript Engine Remote Code Execution Vulnerability". Esto afecta a Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10 y Windows 10 Servers.

Ocurrencias: 8

Hosts afectados: 7

Paquete: vbscript-engine

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2018-8174

CVE-2017-0144

Detalle técnico: El servidor SMBv1 en Microsoft Windows Vista SP2; Windows Server 2008 SP2 y R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold y R2; Windows RT 8.1; y Windows 10 Gold, 1511 y 1607; y Windows Server 2016 permite a atacantes remotos ejecutar código arbitrario a través de paquetes manipulados, vulnerabilidad también conocida como "Windows SMB Remote Code Execution Vulnerability". Esta vulnerabilidad es diferente a la descrita en CVE-2017-0143, CVE-2017-0145, CVE-2017-0146 y CVE-2017-0148.

Ocurrencias: 9

Hosts afectados: 8

Paquete: smb-server

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2017-0144

CVE-2021-44228

Detalle técnico: Las características JNDI de Apache Log4j2 2.0-beta9 hasta 2.15.0 (excluyendo las versiones de seguridad 2.12.2, 2.12.3 y 2.3.1) utilizadas en la configuración, los mensajes de registro y los parámetros no protegen contra LDAP controlado por un atacante y otros puntos finales relacionados con JNDI. Un atacante que pueda controlar los mensajes de registro o los parámetros de los mensajes de registro puede ejecutar código arbitrario cargado desde servidores LDAP cuando la sustitución de la búsqueda de mensajes está habilitada. A partir de la versión 2.15.0 de log4j, este comportamiento ha sido...

Ocurrencias: 3

Hosts afectados: 3

Paquete: log4j-core

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-44228

CVE-2023-23397

Detalle técnico: Microsoft Outlook Elevation of Privilege Vulnerability

Ocurrencias: 8

Hosts afectados: 8

Paquete: outlook

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-23397

CVE-2018-11776

Detalle técnico: Apache Struts, desde la versión 2.3 hasta la 2.3.34 y desde la versión 2.5 hasta la 2.5.16, sufre de una posible ejecución remota de código cuando el valor de alwaysSelectFullNamespace es "true" (establecido por el usuario o por un plugin como Convention Plugin). Además, los resultados se emplean sin ningún espacio de nombres y, al mismo tiempo, el paquete superior no tiene espacio de nombres o contiene caracteres comodín. De manera similar a como pasa con los resultados, existe la misma posibilidad al emplear la etiqueta url, que no tiene un valor y acción definidos y, además, su paquete s...

Ocurrencias: 6

Hosts afectados: 4

Paquete: apache-struts

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2018-11776

CVE-2023-28432

Detalle técnico: Minio is a Multi-Cloud Object Storage framework. In a cluster deployment starting with RELEASE.2019-12-17T23-16-33Z and prior to RELEASE.2023-03-20T20-16-18Z, MinIO returns all environment variables, including `MINIO_SECRET_KEY` and `MINIO_ROOT_PASSWORD`, resulting in information disclosure. All users of distributed deployment are impacted. All users are advised to upgrade to RELEASE.2023-03-20T20-16-18Z.

Ocurrencias: 7

Hosts afectados: 7

Paquete: office

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-28432

CVE-2022-3602

Detalle técnico: Puede activarse una saturación del búfer en la verificación del certificado X.509, específicamente en la verificación de restricciones en el nombre. Tenga en cuenta que esto ocurre después de la verificación de la firma de la cadena de certificados y requiere que una CA haya firmado el certificado malicioso o que la aplicación continúe con la verificación del certificado a pesar de no poder construir una ruta a un emisor confiable. Un atacante puede crear una dirección de correo electrónico maliciosa para desbordar cuatro bytes en la pila de memoria controlados por el atacante. Este desbord...

Ocurrencias: 5

Hosts afectados: 5

Paquete: openssl

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-3602

Vulnerabilidades Bajas

CVE-2023-36884

Detalle técnico: Windows Search Remote Code Execution Vulnerability

Ocurrencias: 5

Hosts afectados: 5

Paquete: windows-kernel

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-36884

CVE-2021-26857

Detalle técnico: Una Vulnerabilidad de Ejecución de código remota de Microsoft Exchange Server. Este ID de CVE es diferente de CVE-2021-26412, CVE-2021-26854, CVE-2021-26855, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078

Ocurrencias: 2

Hosts afectados: 2

Paquete: exchange-deserializer

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-26857

CVE-2024-21338

Detalle técnico: Vulnerabilidad de elevación de privilegios del kernel de Windows

Ocurrencias: 1

Hosts afectados: 1

Paquete: minio

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2024-21338

CVE-2018-11776

Detalle técnico: Apache Struts, desde la versión 2.3 hasta la 2.3.34 y desde la versión 2.5 hasta la 2.5.16, sufre de una posible ejecución remota de código cuando el valor de alwaysSelectFullNamespace es "true" (establecido por el usuario o por un plugin como

Convention Plugin). Además, los resultados se emplean sin ningún espacio de nombres y, al mismo tiempo, el paquete superior no tiene espacio de nombres o contiene caracteres comodín. De manera similar a como pasa con los resultados, existe la misma posibilidad al emplear la etiqueta url, que no tiene un valor y acción definidos y, además, su paquete s...

Ocurrencias: 2

Hosts afectados: 2

Paquete: apache-struts

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2018-11776

CVE-2020-1472

Detalle técnico: Se presenta una vulnerabilidad de elevación de privilegios cuando un atacante establece una conexión de canal seguro Netlogon vulnerable hacia un controlador de dominio, usando el Netlogon Remote Protocol (MS-NRPC), también se conoce como "Netlogon Elevation of Privilege Vulnerability".

Ocurrencias: 3

Hosts afectados: 3

Paquete: netlogon

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2020-1472

CVE-2022-1388

Detalle técnico: En F5 BIG-IP versiones 16.1.x anteriores a 16.1.2.2, versiones 15.1.x anteriores a 15.1.5.1, versiones 14.1.x anteriores a 14.1.4.6, versiones 13.1.x anteriores a 13.1.5 y todas las versiones 12.1.x y 11.6.x, las peticiones no reveladas pueden omitir la autenticación REST de iControl. Nota: las versiones de software que han alcanzado el Fin del Soporte Técnico (EoTS) no son evaluadas

Ocurrencias: 4

Hosts afectados: 3

Paquete: f5-bigip

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-1388

CVE-2021-44228

Detalle técnico: Las características JNDI de Apache Log4j2 2.0-beta9 hasta 2.15.0 (excluyendo las versiones de seguridad 2.12.2, 2.12.3 y 2.3.1) utilizadas en la configuración, los mensajes de registro y los parámetros no protegen contra LDAP controlado por un atacante y otros puntos finales relacionados con JNDI. Un atacante que pueda controlar los mensajes de registro o los parámetros de los mensajes de registro puede ejecutar código arbitrario cargado desde servidores LDAP cuando la sustitución de la búsqueda de mensajes está habilitada. A partir de la versión 2.15.0 de log4j, este comportamiento ha sido...

Ocurrencias: 3

Hosts afectados: 3

Paquete: log4j-core

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-44228

CVE-2019-0708

Detalle técnico: Existe una vulnerabilidad de ejecución remota de código en Remote Desktop Services, anteriormente conocido como Terminal Services, cuando un atacante no autenticado se conecta al sistema de destino mediante RDP y envía peticiones especialmente diseñadas, conocida como 'Remote Desktop Services Remote Code Execution Vulnerability'.

Ocurrencias: 3

Hosts afectados: 3

Paquete: rdp-service

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2019-0708

CVE-2023-41064

Detalle técnico: Se solucionó un problema de Desbordamiento de Búfer de manejo de la memoria mejorada. Este problema se solucionó en macOS Monterey 12.6.9, macOS Big Sur 11.7.10, macOS Ventura 13.5.2, iOS 16.6.1 y iPadOS 16.6.1, iOS 15.7.9 y iPadOS 15.7.9. El procesamiento de una imagen creada con fines maliciosos puede provocar la ejecución de código arbitrario. Apple está al tanto de un informe de que este problema puede haber sido explotado activamente.

Ocurrencias: 4

Hosts afectados: 4

Paquete: imessage

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-41064

CVE-2022-3602

Detalle técnico: Puede activarse una saturación del búfer en la verificación del certificado X.509, específicamente en la verificación de restricciones en el nombre. Tenga en cuenta que esto ocurre después de la verificación de la firma de la cadena de certificados y requiere que una CA haya firmado el certificado malicioso o que la aplicación continúe con la verificación del certificado a pesar de no poder construir una ruta a un emisor confiable. Un atacante puede crear una dirección de correo electrónico maliciosa para desbordar cuatro bytes en la pila de memoria controlados por el atacante. Este desbord...

Ocurrencias: 3

Hosts afectados: 3

Paquete: openssl

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-3602

CVE-2019-19781

Detalle técnico: Se descubrió un problema en Citrix Application Delivery Controller (ADC) and Gateway versiones 10.5, 11.1, 12.0, 12.1 y 13.0. Permiten un salto de directorio.

Ocurrencias: 3

Hosts afectados: 3

Paquete: citrix-adc

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2019-19781

CVE-2021-21985

Detalle técnico: VSphere Client (HTML5) contiene una vulnerabilidad de ejecución de código remota debido a una falta de comprobación de entrada en el plugin Virtual SAN Health Check, que está habilitado por defecto en vCenter Server. Un actor malicioso con acceso de red al puerto 443 puede explotar este problema para ejecutar comandos con privilegios ilimitados en el sistema operativo subyacente que aloja a vCenter Server

Ocurrencias: 4

Hosts afectados: 4

Paquete: vmware-vcenter

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-21985

CVE-2017-0144

Detalle técnico: El servidor SMBv1 en Microsoft Windows Vista SP2; Windows Server 2008 SP2 y R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold y R2; Windows RT 8.1; y Windows 10 Gold, 1511 y 1607; y Windows Server 2016 permite a atacantes remotos ejecutar código arbitrario a través de paquetes manipulados, vulnerabilidad también conocida como "Windows SMB Remote Code Execution Vulnerability". Esta vulnerabilidad es diferente a la descrita en CVE-2017-0143, CVE-2017-0145, CVE-2017-0146 y CVE-2017-0148.

Ocurrencias: 5

Hosts afectados: 5

Paquete: smb-server

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2017-0144

CVE-2021-34527

Detalle técnico: Una vulnerabilidad en la ejecución de código remota de Windows Print Spooler

Ocurrencias: 1

Hosts afectados: 1

Paquete: print-spooler

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-34527

CVE-2021-34523

Detalle técnico: Una vulnerabilidad de Elevación de Privilegios de Microsoft Exchange Server. Este ID de CVE es diferente de CVE-2021-33768, CVE-2021-34470

Ocurrencias: 2

Hosts afectados: 2

Paquete: exchange-elev

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-34523

CVE-2020-0601

Detalle técnico: Se presenta una vulnerabilidad de suplantación de identidad en la manera en que Windows CryptoAPI (Crypt32.dll) comprueba los certificados Elliptic Curve Cryptography (ECC). Un atacante podría explotar la vulnerabilidad mediante el uso de un certificado de firma de código falsificado para firmar un ejecutable malicioso, haciendo que parezca que el archivo era de una fuente confiable y legítima, también se conoce como "Windows CryptoAPI Spoofing Vulnerability".

Ocurrencias: 1

Hosts afectados: 1

Paquete: windows-cryptoapi

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2020-0601

CVE-2024-30088

Detalle técnico: Vulnerabilidad de elevación de privilegios del kernel de Windows

Ocurrencias: 3

Hosts afectados: 3

Paquete: tpm-driver

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2024-30088

CVE-2022-22965

Detalle técnico: Una aplicación Spring MVC o Spring WebFlux que es ejecutada en JDK 9+ puede ser vulnerable a la ejecución de código remota (RCE) por medio de una vinculación de datos. La explotación específica requiere que la aplicación sea ejecutada en Tomcat como un despliegue WAR. Si la aplicación es desplegada como un jar ejecutable de Spring Boot, es decir, por defecto, no es vulnerable a la explotación. Sin embargo, la naturaleza de la vulnerabilidad es más general, y puede haber otras formas de explotarla

Ocurrencias: 2

Hosts afectados: 2

Paquete: spring-framework

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-22965

CVE-2023-4863

Detalle técnico: El desbordamiento del búfer de memoria en libwebp en Google Chrome anterior a 116.0.5845.187 y libwebp 1.3.2 permitía a un atacante remoto realizar una escritura en memoria fuera de los límites a través de una página HTML manipulada. (Severidad de seguridad de Chromium: crítica)

Ocurrencias: 1

Hosts afectados: 1

Paquete: chrome

Referencia: https://nvd.nist.gov/vuln/detail/CVE-2023-4863