Boletín de Seguridad Informática

Vulnerabilidades de Microsoft Exchange

Descripción breve

Boletín informativo sobre vulnerabilidades presentes en los servidores de correo electrónico Microsoft Exchange

Ing. César Alejandro Varela Cruz

Ing. Andrés Martínez López

M.I. Adriana Cruz García

csi.incidentes@unam.mx

Evaluado por:
Ing. Julio César Roldán Elorza

Avalado por:
M. en C. Carlos R. Tlahuel Pérez

Contenido

Resumen Ejecutivo

Este boletín tiene como objetivo proporcionar una visión general sobre las vulnerabilidades asociadas a la tecnología **"Microsoft Exchange 2010",** utilizada por miles de usuarios alrededor del mundo. Esta tecnología ha sido objeto de múltiples vulnerabilidades a lo largo del tiempo, que han afectado la Confidencialidad, Integridad y/o disponibilidad de la información, servicios o sistemas en general alrededor del mundo.

Puntos clave:

1. **Descripción General de las Vulnerabilidades:** Microsoft Exchange 2010 ha sido objeto de múltiples vulnerabilidades que han comprometido su funcionalidad, la seguridad de los sistemas y la información de los usuarios que lo utilizan. Entre las vulnerabilidades expuestas más destacables de incluyen, ejecución de código remoto, elevación de privilegios y exposición de información de manera no errónea y/o no autorizada.

2. **Impacto en la Seguridad:** Las vulnerabilidades en Microsoft Exchange 2010 pueden llegar a permitir a los atacantes ejecutar código malicioso en los servidores afectados, acceder a información confidencial y comprometer la integridad del sistema. El uso de esta versión de esta tecnología expone a una gran cantidad de organizaciones a riesgos significativos.

3. **Medidas de Mitigación Recomendadas:**

    - **Actualización de Versiones**: Es fundamental que las organizaciones actualicen a la última versión estable de Microsoft Exchange ya que esta debe contar con las ultimas actualizaciones o parches de seguridad.

    - **Revisión de Configuraciones**: Revisar y ajustar las configuraciones del servidor a la forma más restrictiva que permita el modelo de negocio, con el fin de minimizar riesgos sin afectar significativamente la funcionalidad o experiencia de usuario.

    - **Monitoreo Activo**: Implementar sistemas de monitoreo para detectar actividades sospechosas que podrían indicar intentos de explotación de vulnerabilidades.

4. **Recomendaciones de Seguridad:**

    - **Realizar Auditorías de Seguridad**: Ejecutar auditorías y pruebas de penetración de manera regular para identificar y mitigar vulnerabilidades en el sistema.

    - **Capacitación y Concientización**: Capacitar a los administradores y al personal de TI sobre las mejores prácticas de seguridad y la importancia de aplicar actualizaciones de manera oportuna.

Conclusión: Las vulnerabilidades presentes en las versiones de Microsoft Exchange 2010 representan un gran riesgo para la seguridad de los sistemas que lo implementan. Es crucial que las organizaciones tomen las medidas de mitigación recomendadas, mantengan actualizada la versión

de esta tecnología y refuercen sus prácticas de seguridad para protegerse contra posibles agentes maliciosos.

Artículo Principal

Dentro de la Universidad Nacional Autónoma de México existe una gran variedad de activos distribuidos en múltiples servidores y dependencias. La existencia de cientos de sistemas diseñados por la universidad, la falta de unificación en ellos y de equipos de TI encargados de mantenimiento de los sistemas en cada una de las dependencias, dan como resultado que existan sistemas legacy o incluso sistemas obsoletos que no han sido eliminados lo que puede causar la presencia de múltiples vulnerabilidades.

Se han identificado múltiples servidores dentro de la red de la UNAM (Consultar Anexo III) que cuentan con versiones desactualizadas de Microsoft Exchange como servidor de correo. Si bien mediante un análisis externo no es posible identificar la subversión exacta de Microsoft Exchange implementada, sin embargo, basado en las firmas obtenidas por el servidor se puede identificar la versión Microsoft Exchange 2010.

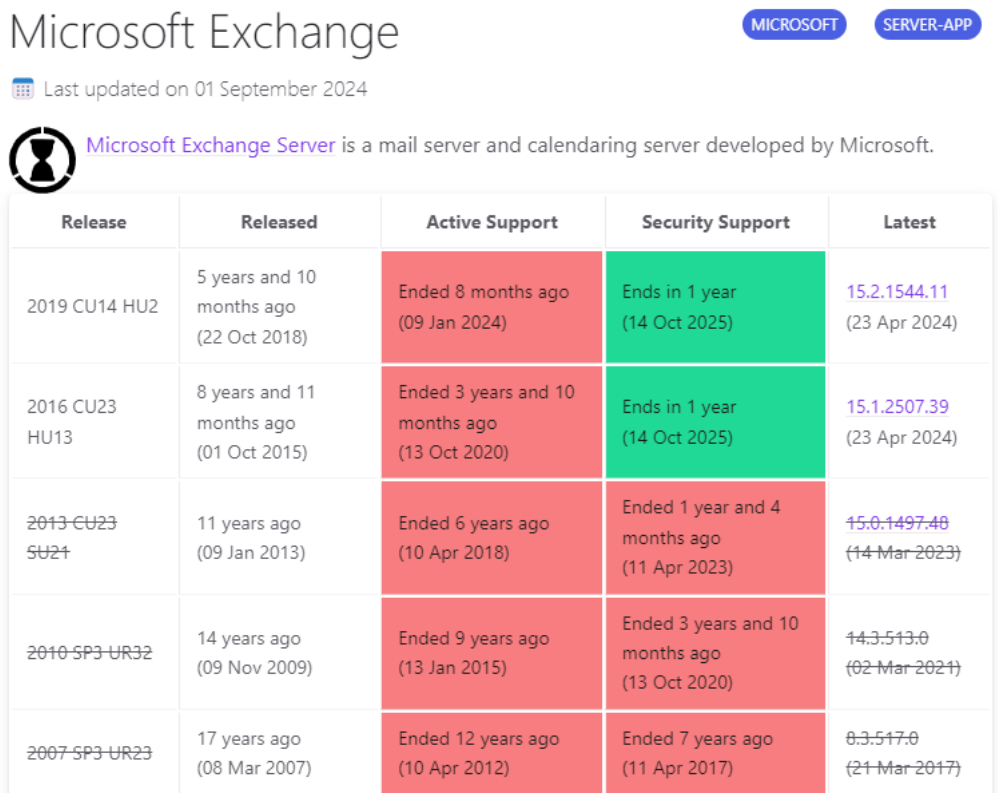
El ciclo de vida del software es una metodología que define la serie de pasos que deben seguirse al momento de realizar un desarrollo de software. Estos pasos abarcan desde el análisis de los requerimientos, diseño, codificación y pruebas hasta el despliegue, e incluso el mantenimiento. Usualmente las compañías que desarrollan el software suelen solucionar los pequeños bugs o vulnerabilidades o inclusive agregar nuevas funcionalidades a través de parches, lo que suele dar como resultado una nueva versión menor.

Imagen 1 Ciclo de vida del software

Cuando un software contiene una nueva funcionalidad muy significativa, se han modificado características claves de la funcionalidad o inclusive se llega a modificar gran parte del código fuente debido a una vulnerabilidad suele surgir una versión mayor lo cual la mayoría de las veces implica

que la versión anterior deje de tener soporte dejando a los usuarios de estas tecnologías obsoletas vulnerables a los problemas, a esto se le conoce como fin del ciclo de vida del software.

Como se puede observar en la siguiente imagen, el ciclo de vida de Microsoft Exchange terminó oficialmente el 13 de octubre del 2020, siendo esta la fecha en la que se dejaron de lanzar nuevos parches de seguridad, sin embargo, se puede observar que el soporte activo a este software terminó más de 5 años antes.



Microsoft Exchange

MICROSOFT SERVER-APP

Last updated on 01 September 2024

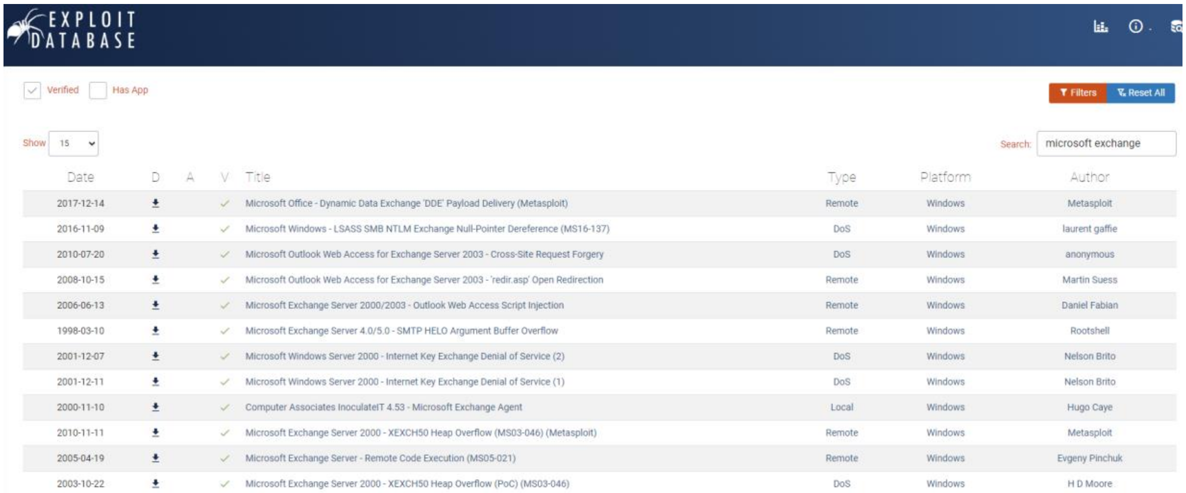
Microsoft Exchange Server is a mail server and calendaring server developed by Microsoft.

Release	Released	Active Support	Security Support	Latest
2019 CU14 HU2	5 years and 10 months ago (22 Oct 2018)	Ended 8 months ago (09 Jan 2024)	Ends in 1 year (14 Oct 2025)	15.2.1544.11 (23 Apr 2024)
2016 CU23 HU13	8 years and 11 months ago (01 Oct 2015)	Ended 3 years and 10 months ago (13 Oct 2020)	Ends in 1 year (14 Oct 2025)	15.1.2507.39 (23 Apr 2024)
~~2013 CU23 SU21~~	11 years ago (09 Jan 2013)	Ended 6 years ago (10 Apr 2018)	Ended 1 year and 4 months ago (11 Apr 2023)	~~15.0.1497.48 (14 Mar 2023)~~
~~2010 SP3 UR32~~	14 years ago (09 Nov 2009)	Ended 9 years ago (13 Jan 2015)	Ended 3 years and 10 months ago (13 Oct 2020)	~~14.3.513.0 (02 Mar 2021)~~
~~2007 SP3 UR23~~	17 years ago (08 Mar 2007)	Ended 12 years ago (10 Apr 2012)	Ended 7 years ago (11 Apr 2017)	~~8.3.517.0 (21 Mar 2017)~~

Imagen 2 Ciclo de vida de Microsoft Exchange

Es importante destacar que el hecho de que un software sea legítimo y respaldado por una gran empresa como es Microsoft, no está exento de contar con vulnerabilidades que podrían representar un alto riesgo para los servidores, sin embargo, el hecho de que un software se encuentre respaldado por una empresa o una gran comunidad usualmente aumenta la eficacia al resolver o parchar estas vulnerabilidades, por lo que es importante mantener la última versión estable del software utilizado.

Hoy en día, existen múltiples exploits públicos en la red, considerados como disponibles para poder realizar la prueba de concepto bajo el supuesto de que esta vulnerabilidad ya fue parchada, sin embargo, hay ocasiones en las que no se cuentan con licencias o simplemente a falta de ventanas de mantenimiento, no se actualizan los servidores ya que esto podría implicar en algunas ocasiones el hecho de que se deba reiniciar el servidor, lo que en ocasiones implica interrumpir el servicio.



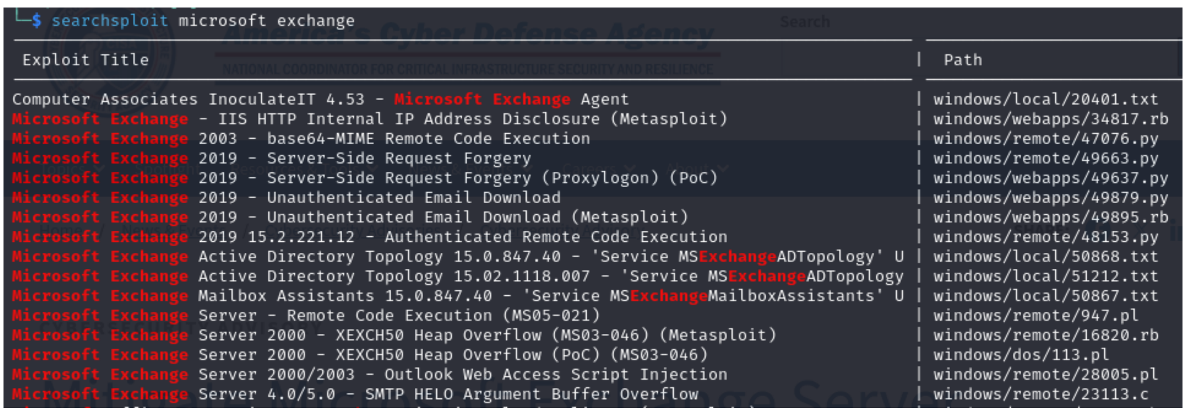
EXPLOIT DATABASE

Verified Has App Filters Reset All

Show 15 Search: microsoft exchange

Date	D	A	V	Title	Type	Platform	Author
2017-12-14			✓	Microsoft Office - Dynamic Data Exchange 'DDE' Payload Delivery (Metasploit)	Remote	Windows	Metasploit
2016-11-09			✓	Microsoft Windows - LSASS SMB NTLM Exchange Null-Pointer Dereference (MS16-137)	DoS	Windows	laurent gaffie
2010-07-20			✓	Microsoft Outlook Web Access for Exchange Server 2003 - Cross-Site Request Forgery	DoS	Windows	anonymous
2008-10-15			✓	Microsoft Outlook Web Access for Exchange Server 2003 - 'redir.asp' Open Redirection	Remote	Windows	Martin Suess
2006-06-13			✓	Microsoft Exchange Server 2000/2003 - Outlook Web Access Script Injection	Remote	Windows	Daniel Fabian
1998-03-10			✓	Microsoft Exchange Server 4.0/5.0 - SMTP HELO Argument Buffer Overflow	Remote	Windows	Rootshell
2001-12-07			✓	Microsoft Windows Server 2000 - Internet Key Exchange Denial of Service (2)	DoS	Windows	Nelson Brito
2001-12-11			✓	Microsoft Windows Server 2000 - Internet Key Exchange Denial of Service (1)	DoS	Windows	Nelson Brito
2000-11-10			✓	Computer Associates InoculateIT 4.53 - Microsoft Exchange Agent	Local	Windows	Hugo Caye
2010-11-11			✓	Microsoft Exchange Server 2000 - XEXCH50 Heap Overflow (MS03-046) (Metasploit)	Remote	Windows	Metasploit
2005-04-19			✓	Microsoft Exchange Server - Remote Code Execution (MS05-021)	Remote	Windows	Evgeny Pinchuk
2003-10-22			✓	Microsoft Exchange Server 2000 - XEXCH50 Heap Overflow (PoC) (MS03-046)	DoS	Windows	H D Moore

Imagen 3 Exploits disponibles en Exploit-DB

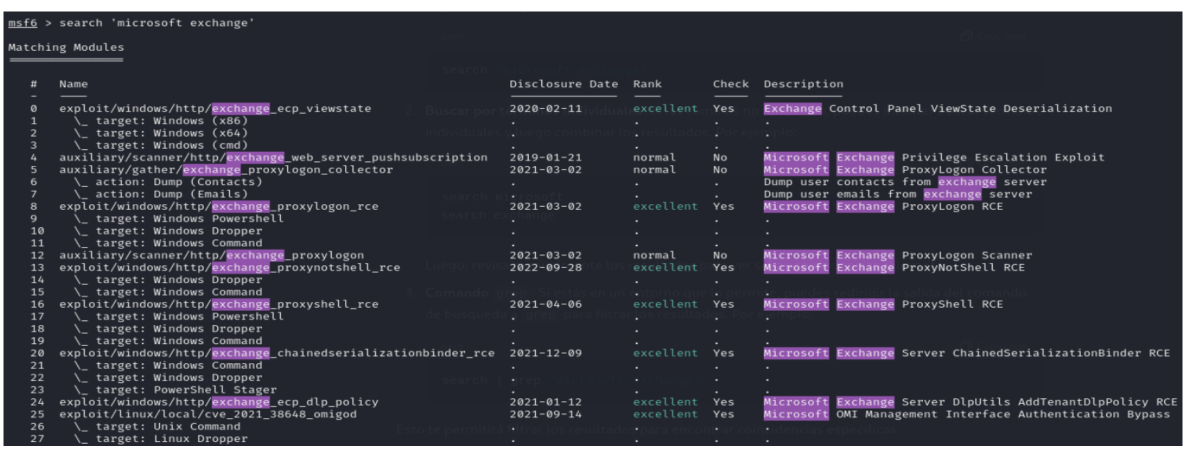


```
└─$ searchsploit microsoft exchange

 Exploit Title                                                                   |  Path

Computer Associates InoculateIT 4.53 - Microsoft Exchange Agent                  | windows/local/20401.txt
Microsoft Exchange - IIS HTTP Internal IP Address Disclosure (Metasploit)        | windows/webapps/34817.rb
Microsoft Exchange 2003 - base64-MIME Remote Code Execution                      | windows/remote/47076.py
Microsoft Exchange 2019 - Server-Side Request Forgery                            | windows/remote/49663.py
Microsoft Exchange 2019 - Server-Side Request Forgery (Proxylogon) (PoC)         | windows/webapps/49637.py
Microsoft Exchange 2019 - Unauthenticated Email Download                         | windows/webapps/49879.py
Microsoft Exchange 2019 - Unauthenticated Email Download (Metasploit)            | windows/webapps/49895.rb
Microsoft Exchange 2019 15.2.221.12 - Authenticated Remote Code Execution        | windows/remote/48153.py
Microsoft Exchange Active Directory Topology 15.0.847.40 - 'Service MSExchangeADTopology' U | windows/local/50868.txt
Microsoft Exchange Active Directory Topology 15.02.1118.007 - 'Service MSExchangeADTopology | windows/local/51212.txt
Microsoft Exchange Mailbox Assistants 15.0.847.40 - 'Service MSExchangeMailboxAssistants' U | windows/local/50867.txt
Microsoft Exchange Server - Remote Code Execution (MS05-021)                     | windows/remote/947.pl
Microsoft Exchange Server 2000 - XEXCH50 Heap Overflow (MS03-046) (Metasploit)   | windows/remote/16820.rb
Microsoft Exchange Server 2000 - XEXCH50 Heap Overflow (PoC) (MS03-046)          | windows/dos/113.pl
Microsoft Exchange Server 2000/2003 - Outlook Web Access Script Injection        | windows/remote/28005.pl
Microsoft Exchange Server 4.0/5.0 - SMTP HELO Argument Buffer Overflow           | windows/remote/23113.c
```

Imagen 4 Exploits disponibles con el comando searchsploit



```
msf6 > search 'microsoft exchange'

Matching Modules
================

   #   Name                                                      Disclosure Date  Rank       Check  Description
   -   ----                                                      ---------------  ----       -----  -----------
   0   exploit/windows/http/exchange_ecp_viewstate               2020-02-11       excellent  Yes    Exchange Control Panel ViewState Deserialization
   1     \_ target: Windows (x86)                                .                .          .      .
   2     \_ target: Windows (x64)                                .                .          .      .
   3     \_ target: Windows (cmd)                                .                .          .      .
   4   auxiliary/scanner/http/exchange_web_server_pushsubscription  2019-01-21    normal     No     Microsoft Exchange Privilege Escalation Exploit
   5   auxiliary/gather/exchange_proxylogon_collector            2021-03-02       normal     No     Microsoft Exchange ProxyLogon Collector
   6     \_ action: Dump (Contacts)                              .                .          .      Dump user contacts from exchange server
   7     \_ action: Dump (Emails)                                .                .          .      Dump user emails from exchange server
   8   exploit/windows/http/exchange_proxylogon_rce              2021-03-02       excellent  Yes    Microsoft Exchange ProxyLogon RCE
   9     \_ target: Windows Powershell                           .                .          .      .
   10    \_ target: Windows Dropper                              .                .          .      .
   11    \_ target: Windows Command                              .                .          .      .
   12  auxiliary/scanner/http/exchange_proxylogon                2021-03-02       normal     No     Microsoft Exchange ProxyLogon Scanner
   13  exploit/windows/http/exchange_proxynotshell_rce           2022-09-28       excellent  Yes    Microsoft Exchange ProxyNotShell RCE
   14    \_ target: Windows Dropper                              .                .          .      .
   15    \_ target: Windows Command                              .                .          .      .
   16  exploit/windows/http/exchange_proxyshell_rce              2021-04-06       excellent  Yes    Microsoft Exchange ProxyShell RCE
   17    \_ target: Windows Powershell                           .                .          .      .
   18    \_ target: Windows Dropper                              .                .          .      .
   19    \_ target: Windows Command                              .                .          .      .
   20  exploit/windows/http/exchange_chainedserializationbinder_rce  2021-12-09   excellent  Yes    Microsoft Exchange Server ChainedSerializationBinder RCE
   21    \_ target: Windows Command                              .                .          .      .
   22    \_ target: Windows Dropper                              .                .          .      .
   23    \_ target: PowerShell Stager                            .                .          .      .
   24  exploit/windows/http/exchange_ecp_dlp_policy              2021-01-12       excellent  Yes    Microsoft Exchange Server DlpUtils AddTenantDlpPolicy RCE
   25  exploit/linux/local/cve_2021_38648_omigod                 2021-09-14       excellent  Yes    Microsoft OMI Management Interface Authentication Bypass
   26    \_ target: Unix Command                                 .                .          .      .
   27    \_ target: Linux Dropper                                .                .          .      .
```

Imagen 5 Exploits disponibles en Metasploit

Como se observa en las imágenes anteriores prácticamente cualquier base de datos de exploits posee hoy en día exploits de algunas versiones de Microsoft Exchange.

Analizando algunos de los exploits disponibles para las vulnerabilidades más importantes de Microsoft Exchange en exploit-db, uno de los principales repositorios de exploits, se puede observar como muchos de estos se aprovechan de la validación impropia de las entradas de los usuarios (CWE-20) para poder inyectar código en lenguajes como powershell. De esta manera, al lograr ejecutar código de manera remota en el servidor es posible escalar el ataque creando una Shell y posteriormente movimiento lateral.

Algunas de los exploits poseen la carga útil codificada para evitar ser eliminados por los antivirus, de igual manera algunos exploits aprovechan la debilidad del servidor de no realizar correctamente la verificación de las credenciales de los usuarios, por lo que ni siquiera son necesarias para ejecutar código para extraer o inyectar información en general del servidor como pueden ser, direcciones de correo electrónico, contenido de los correos, información de los dueños de las cuentas, información del servidor, entre otras.

```
def get_ip_extract
  urls = ["/Microsoft-Server-ActiveSync/default.eas",
    "/Microsoft-Server-ActiveSync",
    "/Autodiscover/Autodiscover.xml",
    "/Autodiscover",
    "/Exchange",
    "/Rpc",
    "/EWS/Exchange.asmx",
    "/EWS/Services.wsdl",
    "/EWS",
    "/ecp",
    "/OAB",
    "/OWA",
    "/aspnet_client",
    "/PowerShell"]

  result = nil

  urls.each do |url|
    begin
      res = send_request_cgi({
        'version' => "1.0",
        'uri'     => "#{url}",
        'method'  => 'GET',
        'vhost'  =>  ''
      }, timeout = datastore['TIMEOUT'])

    rescue ::Rex::ConnectionError, Errno::ECONNREFUSED, Errno::ETIMEDOUT
      print_error("#{msg} HTTP Connection Failed")
      next
    end

    if not res
      print_error("#{msg} HTTP Connection Timeout")
      next
    end

    if res and res.code == 401 and (match = res['WWW-Authenticate'].match(/Basic realm=\"(192\.168\.[0-9]{1,3}\.[0-9]{1,3}|10\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}|172\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})\"/i))
      result = match.captures[0]
      print_status("#{msg} Status Code: 401 response")
      print_status("#{msg} Found Path: " + url )
      print_good("#{msg} Found target internal IP address: " + result)
      return result
     elseif
      print_warning("#{msg} No internal address found")
      next
    end
```

Imagen 6 Exploit para obtención de la dirección IP interna en IIS HTTP

A continuación, se muestran algunas noticias que muestran el alcance y el impacto que han tenido las vulnerabilidades de Microsoft Exchange alrededor del mundo.

Noticias de Ciberseguridad

Un ciberataque a Microsoft Exchange pone en riesgo a decenas de miles de empresas

Debido a la gran importancia y facilidad de uso que tiene esta herramienta de Microsoft, ha sido utilizado por una gran cantidad de empresas, yendo desde grandes empresas hasta PYMES, abarcando también múltiples sectores como gubernamentales y empresariales alrededor del mundo.

Debido a su amplio uso, esta noticia estima que al menos 30,000 organizaciones podrían ser afectadas alrededor del mundo por un ciberataque dirigido a este software, sin embargo, otras estimaciones sugieren que podrían ser más de 250,000.

De acuerdo con lo reportado en esta noticia, los grupos delictivos accedían y tomaban control completo de los servidores sin necesidad de credenciales, por lo que una gran cantidad de servidores conectados directamente a internet podrían haber sido afectados.

Debido a las características de uso de Microsoft Exchange, los atacantes podían usar el control sobre estos para establecer persistencia en las organizaciones, así como esparcir malware como ransomware a los empleados o personas en general asociadas a estos servidores, a su vez robar información de los correos de las mismas.

La vulnerabilidad de Exchange que compromete los servidores para ataques futuros: cómo funciona y sus posibles parches

Debido a la gravedad de las vulnerabilidades que se han encontrado en Microsoft Exchange, Microsoft se vio en la necesidad de publicar parches de seguridad de manera extraordinaria, además de una herramienta que pudiera implementar estos parches provisionales de manera local de forma sencilla. La herramienta de mitigación local de Microsoft Exchange (EOMT, por sus siglas en inglés Exchange On-Premises Mitigation Tool) permite aplicar los parches de seguridad críticos a través de un solo clic.

La vulnerabilidad CVE-2021-26855 permite realizar un “ataque en cadena” a través de movimiento lateral una vez comprometido el servidor Exchange.

El FBI y la CISA estiman que alrededor de 7,000 servidores fueron comprometidos a lo largo de los Estados Unidos de América.

Esta vulnerabilidad podía afectar a servidores Exchange 2019, 2016, 2013 y 2010.

Consejos Prácticos

Si bien no es posible garantizar la seguridad de un sistema, es posible prevenir y reducir la posibilidad de que un sistema sea explotado, para esto se ofrecen las siguientes recomendaciones.

- Mantener el software actualizado a su última versión estable. Ya que estas versiones normalmente cuentan con todos los parches de seguridad y son menos propensos a bugs de lo que lo sería una versión alfa, beta, etc.
- Implementar una configuración segura del servidor, para esto se puede hacer uso de guías como las CIS Benchmarks.
- Implementar una autenticación de multi-factor, ya que esto agrega seguridad a la cuenta de los usuarios
- Monitorear la red. De ser posible se recomienda monitorear la red de manera activa, preferentemente a través de un SIEM o un SOAR.
- De no ser necesario, se recomienda asilar los servidores Exchange del Internet, es decir, si los usuarios del servidor se conectan de forma local, el servidor puede estar expuesto solamente de forma local.
- Realizar copias de seguridad de manera recurrente, debido a que muchos de los grupos delictivos han utilizado las vulnerabilidades de Microsoft Exchange para esparcir ransomware.
- Proporcionar capacitación al personal.
- Realizar auditorías de seguridad de manera periódica.

Conclusión

Las vulnerabilidades en Microsoft Exchange han demostrado ser un blanco atractivo para los ciberdelincuentes. La rápida evolución de las amenazas cibernéticas exige que las organizaciones no solo apliquen actualizaciones y parches de seguridad de manera oportuna, sino que también implementen prácticas robustas de monitoreo y respuesta ante incidentes, manteniendo una postura de seguridad proactiva.

Existen muchas vulnerabilidades que afectan a Microsoft Exchange (Ver Anexo A), de las cuales, la mayoría actualmente se encuentran parchadas por lo que se recomienda mantener siempre actualizados los servidores ya que como buena práctica es una de las mejores maneras de mantener el sistema seguro. Además, se pueden implementar medidas adicionales como la implementación de un SIEM, que incluya reglas yara a la medida o en su defecto las proporcionadas por una entidad de confianza como por ejemplo Volexity (ver anexo II), VirusTotal, Cisco Talos, SANS Institute, entre otros.

A medida que el panorama de amenazas continúa evolucionando, la colaboración dentro de la comunidad de ciberseguridad y el intercambio de información se vuelven esenciales para combatir las vulnerabilidades y asegurar un entorno digital más seguro.

Bibliografía

America's Cyber Defense Agency. (19 de Julio de 2021). *Mitigar las vulnerabilidades de Microsoft Exchange Server*. Obtenido de https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-062a

Aver, H. (10 de Marzo de 2021). *MS Exchange Server y la explotación masiva de sus vulnerabilidades*. Obtenido de https://www.kaspersky.es/blog/exchange-vulnerabilities/24847/

endoflife.date. (01 de Septiembre de 2024). *endoflife.date*. Obtenido de Microsoft Exchange: https://endoflife.date/msexchange

Jiménez, M. (10 de Marzo de 2021). *Cinco Días*. Obtenido de Un ciberataque a Microsoft Exchange pone en riesgo a decenas de miles de empresas: https://cincodias.elpais.com/cincodias/2021/03/10/companias/1615411159_242097.html

Microsoft. (21 de Febrero de 2023). *Exchange architecture*. Obtenido de https://learn.microsoft.com/en-us/exchange/architecture/architecture?view=exchserver-2019

Microsoft. (15 de Agosto de 2023). *Exchange Server build numbers and release dates*. Obtenido de https://learn.microsoft.com/en-us/exchange/new-features/build-numbers-and-release-dates?view=exchserver-2019#exchange-server-2010

Moorcraft, B. (13 de Mayo de 2021). *Microsoft Exchange attacks: How to mitigate and respond to zero-day vulnerabilities*. Obtenido de https://www.insurancebusinessmag.com/us/news/cyber/microsoft-exchange-attacks-how-to-mitigate-and-respond-to-zeroday-vulnerabilities-255001.aspx

Anexo I. Tabla de CVE's reportados que afectan a los servidores Exchange 2010.

Existen múltiples vulnerabilidades relacionadas con la tecnología Exchange 2010, las cuales pueden van desde exposición de información, hasta acceso remoto al servidor. Para algunas de estas vulnerabilidades existen exploits públicos, lo que en algunos casos provocó que múltiples grupos APT's conocidos alrededor del mundo los utilizaran para comprometer servidores. En la siguiente tabla se resumen las principales vulnerabilidades que afectan a la tecnología Exchange 2010.

CVE	Fecha de publicación	Ultima actualización	CVSS	EPSS	Exploits Públicos	Resumen del CVE	Exploit conocido	Usado para ransomware	Tipo de Vulnerabilidad
CVE-2018-8154	09/05/2018	24/08/2020	10	9.97%		A remote code execution vulnerability exists in Microsoft Exchange software when the software fails to properly handle objects in memory, aka "Microsoft Exchange Memory Corruption Vulnerability." This affects Microsoft Exchange Server. This CVE ID is unique from CVE-2018-8151.			RCE
CVE-2018-8302	15/08/2018	24/08/2020	10	54.76%		A remote code execution vulnerability exists in Microsoft Exchange software when the software fails to properly handle objects in memory, aka "Microsoft Exchange Memory Corruption Vulnerability." This affects Microsoft Exchange Server.			RCE
CVE-2019-0724	05/03/2019	24/08/2020	9.3	6.98%	Si	An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka 'Microsoft Exchange Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0686.			Privilege Elevation
CVE-2020-0688	11/02/2020	13/02/2024	9	97.07%	Si	A remote code execution vulnerability exists in Microsoft Exchange software when the software fails to properly handle objects in memory, aka 'Microsoft Exchange Memory Corruption Vulnerability'.	Exploit conocido	Usado para ransomware	RCE
CVE-2020-17144	10/12/2020	26/07/2024	8.8	32.40%		Microsoft Exchange Remote Code Execution Vulnerability	Exploit conocido		RCE

CVE-2018-16793	21/09/2018	20/11/2018	8.6	0.55%		Rollup 18 for Microsoft Exchange Server 2010 SP3 and previous versions has an SSRF vulnerability via the username parameter in /owa/auth/logon.aspx in the OWA (Outlook Web Access) login page.			SSRF
CVE-2019-1136	15/07/2019	24/08/2020	8.1	0.30%		An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka 'Microsoft Exchange Server Elevation of Privilege Vulnerability'.			Privilege Elevation
CVE-2021-26857	03/03/2021	25/07/2024	7.8	60.41%		Microsoft Exchange Server Remote Code Execution Vulnerability	Exploit conocido	Usado para ransomware	RCE
CVE-2021-26858	03/03/2021	25/07/2024	7.8	18.40%		Microsoft Exchange Server Remote Code Execution Vulnerability	Exploit conocido	Usado para ransomware	RCE
CVE-2018-8581	14/11/2018	09/04/2020	7.4	3.44%		An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka "Microsoft Exchange Server Elevation of Privilege Vulnerability." This affects Microsoft Exchange Server.	Exploit conocido	Usado para ransomware	Privilege Elevation
CVE-2019-0686	05/03/2019	24/08/2020	7.4	0.15%		An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka 'Microsoft Exchange Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0724.			Privilege Elevation
CVE-2018-0924	14/03/2018	24/08/2020	6.5	2.57%		Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 20, Microsoft Exchange Server 2013 Cumulative Update 18, Microsoft Exchange Server 2013 Cumulative Update 19, Microsoft Exchange Server 2013 Service Pack 1, Microsoft Exchange Server 2016 Cumulative Update 7, and Microsoft Exchange Server 2016 Cumulative Update 8 allow an information disclosure vulnerability due to how URL redirects are handled, aka "Microsoft Exchange			Information Disclosure

						Information Disclosure Vulnerability". This CVE is unique from CVE-2018-0941.			
CVE-2019-0588	08/01/2019	24/08/2020	6.5	0.14%		An information disclosure vulnerability exists when the Microsoft Exchange PowerShell API grants calendar contributors more view permissions than intended, aka "Microsoft Exchange Information Disclosure Vulnerability." This affects Microsoft Exchange Server.			Information Disclosure
CVE-2019-1084	15/07/2019	04/05/2020	6.5	0.53%		An information disclosure vulnerability exists when Exchange allows creation of entities with Display Names having non-printable characters. An authenticated attacker could exploit this vulnerability by creating entities with invalid display names, which, when added to conversations, remain invisible. This security update addresses the issue by validating display names upon creation in Microsoft Exchange, and by rendering invalid display names correctly in Microsoft Outlook clients., aka 'Microsoft Exchange Information Disclosure Vulnerability'.			Information Disclosure
CVE-2018-0940	14/03/2018	24/08/2020	6.5	0.30%		Microsoft Exchange Outlook Web Access (OWA) in Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 20, Microsoft Exchange Server 2013 Cumulative Update 18, Microsoft Exchange Server 2013 Cumulative Update 19, Microsoft Exchange Server 2013 Service Pack 1, Microsoft Exchange Server 2016 Cumulative Update 7, and Microsoft Exchange Server 2016 Cumulative Update 8 allows an elevation of			Privilege Elevation

						privilege vulnerability due to how links in the body of an email message are rewritten, aka "Microsoft Exchange Elevation of Privilege Vulnerability".			
CVE-2010-1689	07/05/2010	09/04/2020	6.4	0.99%		The DNS implementation in smtpsvc.dll before 6.0.2600.5949 in Microsoft Windows 2000 SP4 and earlier, Windows XP SP3 and earlier, Windows Server 2003 SP2 and earlier, Windows Server 2008 SP2 and earlier, Windows Server 2008 R2, Exchange Server 2003 SP3 and earlier, Exchange Server 2007 SP2 and earlier, and Exchange Server 2010 uses predictable transaction IDs that are formed by incrementing a previous ID by 1, which makes it easier for man-in-the-middle attackers to spoof DNS responses, a different vulnerability than CVE-2010-0024 and CVE-2010-0025.			Man In the Middle
CVE-2010-1690	07/05/2010	09/04/2020	6.4	2.05%		The DNS implementation in smtpsvc.dll before 6.0.2600.5949 in Microsoft Windows 2000 SP4 and earlier, Windows XP SP3 and earlier, Windows Server 2003 SP2 and earlier, Windows Server 2008 SP2 and earlier, Windows Server 2008 R2, Exchange Server 2003 SP3 and earlier, Exchange Server 2007 SP2 and earlier, and Exchange Server 2010 does not verify that transaction IDs of responses match transaction IDs of queries, which makes it easier for man-in-the-middle attackers to spoof DNS responses, a different vulnerability than CVE-2010-0024 and CVE-2010-0025.			Man In the Middle

CVE-2017-8621	11/07/2017	17/07/2017	6.1	0.29%		Microsoft Exchange Server 2010 SP3, Exchange Server 2013 SP3, Exchange Server 2013 CU16, and Exchange Server 2016 CU5 allows an open redirect vulnerability that could lead to spoofing, aka "Microsoft Exchange Open Redirect Vulnerability".			Open Redirect
CVE-2019-0817	09/04/2019	09/04/2020	5.8	0.10%		A spoofing vulnerability exists in Microsoft Exchange Server when Outlook Web Access (OWA) fails to properly handle web requests, aka 'Microsoft Exchange Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0858.			Spoofing
CVE-2014-6319	11/12/2014	12/10/2018	5	1.21%		Outlook Web App (OWA) in Microsoft Exchange Server 2007 SP3, 2010 SP3, and 2013 SP1 and Cumulative Update 6 does not properly validate tokens in requests, which allows remote attackers to spoof the origin of e-mail messages via unspecified vectors, aka "Outlook Web App Token Spoofing Vulnerability."			App Token Spoofing (Origin Spoofing)
CVE-2010-0024	14/04/2010	09/04/2020	5	1.80%		The SMTP component in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, and Server 2008 Gold, SP2, and R2, and Exchange Server 2003 SP2, does not properly parse MX records, which allows remote DNS servers to cause a denial of service (service outage) via a crafted response to a DNS MX record query, aka "SMTP Server MX Record Vulnerability."			DOS
CVE-2010-0025	14/04/2010	09/04/2020	5	25.82%		The SMTP component in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, and Server 2008 Gold, SP2, and R2, and Exchange Server 2000 SP3, does not properly allocate memory for SMTP command replies, which allows remote attackers to read fragments of e-mail messages by sending a			Information Disclosure (Fragmentos de Emails)

						series of invalid commands and then sending a STARTTLS command, aka "SMTP Memory Allocation Vulnerability."			
CVE-2018-8151	09/05/2018	03/10/2019	4.3	1.12%		An information disclosure vulnerability exists when Microsoft Exchange improperly handles objects in memory, aka "Microsoft Exchange Memory Corruption Vulnerability." This affects Microsoft Exchange Server. This CVE ID is unique from CVE-2018-8154.			Memory Corruption
CVE-2016-0138	14/09/2016	12/10/2018	4.3	0.30%		Microsoft Exchange Server 2007 SP3, 2010 SP3, 2013 SP1, 2013 Cumulative Update 12, 2013 Cumulative Update 13, 2016 Cumulative Update 1, and 2016 Cumulative Update 2 misparses e-mail messages, which allows remote authenticated users to obtain sensitive Outlook application information by leveraging the Send As right, aka "Microsoft Exchange Information Disclosure Vulnerability."			Remote User Autentication (Information Disclosure)
CVE-2013-5072	11/12/2013	01/06/2019	4.3	72.06%		Cross-site scripting (XSS) vulnerability in Outlook Web Access in Microsoft Exchange Server 2010 SP2 and SP3 and 2013 Cumulative Update 2 and 3 allows remote attackers to inject arbitrary web script or HTML via a crafted URL, aka "OWA XSS Vulnerability."			XSS
CVE-2012-4791	12/12/2012	01/06/2019	3.5	6.94%		Microsoft Exchange Server 2007 SP3 and 2010 SP1 and SP2 allows remote authenticated users to cause a denial of service (Information Store service hang) by subscribing to a crafted RSS feed, aka "RSS Feed May Cause Exchange DoS Vulnerability."			RSS (DOS)

Anexo II. Reglas Yara

Si bien lo más recomendable para corregir estas vulnerabilidades es actualizar a la versión más reciente y estable del software para aplicar todos los parches de seguridad, algunas agencias como Volexity publicaron algunas reglas yara para poder identificar o bloquear los exploits más conocidos como los usados por el grupo China Chopper. A continuación, se muestran algunas de estas reglas yara:

regla webshell_aspx_simpleseesharp: Webshell sin clasificar

```
{
   meta:
      author = "threatintel@volexity.com"
      date = "2021-03-01"
      description = "Un Webshell ASPX simple que permite a un atacante escribir más archivos en el
disco".
      hash = "893cd3583b49cb706b3e55ecb2ed0757b977a21f5c72e041392d1256f31166e2"
   cadenas:
      $header = "<%@ Page Language=\"C#\" %>"
      $body = "<% HttpPostedFile thisFile = Request.Files[0];thisFile.SaveAs(Path.Combine"
   condición:
      $header en 0 y
      $body y
      tamaño de archivo < 1 KB
}
```

regla webshell_aspx_reGeorgTunnel: Webshell Commodity

```
{
   meta:
      author = "threatintel@volexity.com"
      date = "2021-03-01"
      description = "Una variación del webshell del túnel reGeorg"
      hash = "406b680edc9a1bb0e2c7c451c56904857848b5f15570401450b73b232ff38928"
      referencia = "https://github.com/sensepost/reGeorg/blob/master/tunnel.aspx"
   cadenas:
      $s1 = "System.Net.Sockets"
      $s2 =
"System.Text.Encoding.Default.GetString(Convert.FromBase64String(StrTr(Request.Headers.Get"
      // un poco más experimental
      $t1 = ".Split('|')"
      $t2 = "Request.Headers.Get"
      $t3 = ".Substring("
      $t4 = "new Socket("
      $t5 = "IPAddress ip;"
   condición:
```

```
        todos ($s*) o
        todos ($t*)
}
```

regla webshell_aspx_sportsball : Webshell Sin clasificar

```
{
   meta:
      author = "threatintel@volexity.com"
      date = "2021-03-01"
      description = "El webshell SPORTSBALL permite a los atacantes cargar archivos o ejecutar
comandos en el sistema."
      hash = "2fa06333188795110bba14a482020699a96f76fb1ceb80cbfa2df9d3008b5b0a"
   strings:
      $uniq1 = "HttpCookie newcook = new HttpCookie(\"fqrspt\",
HttpContext.Current.Request.Form"
      $uniq2 = "ZN2aDAB4rXsszEvCLrzgcvQ4oi5J1TuiRULlQbYwldE="
      $var1 = "Result.InnerText = string.Empty;"
      $var2 = "newcook.Expires = DateTime.Now.AddDays("
      $var3 = "Sistema.Diagnóstico.Proceso proceso = nuevo Sistema.Diagnóstico.Proceso();"
      $var4 = "proceso.StandardInput.WriteLine(HttpContext.Current.Request.Form[\""
      $var5 = "de lo contrario si (!string.IsNullOrEmpty(HttpContext.Current.Request.Form[\""
      $var6 = "<tipo de entrada=\"enviar\" valor=\"Cargar\" />"
   condición:
      cualquiera de ($uniq*) o
      todos ($var*)
}
```