ALERTA ISH
MICROSOFT EXCHANGE

Exploração ativa de vulnerabilidades em produtos Microsoft Exchange Server

ID: B.21.04.14.A (com base no alerta AA21-062A - CISA - Atualizado)

DATA: terça-feira, 27 de abril de 2021

RESUMO

ALERTA

Foi emitido um alerta para a exploração ativa de vulnerabilidades em produtos Microsoft Exchange Server. A exploração bem-sucedida dessas vulnerabilidades permite que um invasor não autenticado execute código arbitrário em servidores Exchange vulneráveis, permitindo que o invasor obtenha acesso persistente ao sistema, bem como acesso a arquivos e caixas de correio no servidor e a credenciais armazenadas nesse sistema. A exploração bem-sucedida também pode permitir que o invasor comprometa a confiança e a identidade em uma rede vulnerável.

PATCHES

A Microsoft lançou patches para abordar vulnerabilidades no Microsoft Exchange Server. As vulnerabilidades afetam os Microsoft Exchange Servers locais e não são conhecidas por impactar os serviços de email em nuvem do Exchange Online ou Microsoft 365 (anteriormente O365).

O QUE VOCÊ VAI ENCONTRAR NESTE ALERTA

Este alerta inclui táticas, técnicas e procedimentos (TTPs) e os indicadores de comprometimento (IOCs) associados a esta atividade maliciosa. Para se proteger contra essa ameaça, a CISA recomenda que as organizações examinem seus sistemas para os TTPs e usem os IOCs para detectar qualquer atividade maliciosa.

DETALHES TÉCNICOS

A atualização de segurança da Microsoft de abril de 2021 recentemente divulga e atenua vulnerabilidades significativas que afetam o Exchange Server 2016 e 2019 local.

A Microsoft lançou atualizações de segurança para abordar quatro vulnerabilidades no Exchange Server:

- CVE-2021-28310 – Win32k Elevation of Privilege Vulnerability

Esta é a única vulnerabilidade listada como sendo ativamente explorada e corrigida em abril. O bug permite que um invasor aumente os privilégios executando um programa especialmente criado em um sistema alvo (Ex: *Microsoft Exchange*). Isso significa que eles precisarão fazer logon em um sistema ou enganar um usuário legítimo para que execute o código em seu nome. Considerando quem está listado como quem descobriu o bug, provavelmente ele está sendo usado em malwares. Bugs dessa natureza são normalmente combinados com outros bugs, como um bug do navegador ou exploração de PDF, para assumir o controle de um sistema.

- CVE-2021-28480 e CVE-2021-28481 – Microsoft Exchange Server Remote Code Execution Vulnerability

Ambos os CVEs estão listados em um CVSS de 9,8 *(Critical)* e têm descrições idênticas, portanto, ambos são listados aqui. Ambos os bugs de execução de código não são autenticados e não requerem interação do usuário. Como o vetor de ataque está listado como “Rede”, é provável que esses bugs possam ser alterados - pelo menos entre os servidores Exchange. A pontuação CVSS para esses dois bugs é, na verdade, maior do que os bugs do Exchange explorados no início deste ano. Considerando a fonte, e considerando que esses bugs também recebem a classificação de índice de exploração mais alta da Microsoft, presuma que eles eventualmente serão explorados.

- CVE-2021-28329 et al. – Remote Procedure Call Runtime Remote Code Execution Vulnerability

Das 27 CVEs listadas acima, 12 são classificados como crítica, enquanto 15 são classificados como média. Em vulnerabilidades RPC comumente, um invasor precisaria enviar uma solicitação RPC especialmente criada para um sistema previamente infectado. A exploração bem-sucedida resulta na execução de código no contexto de outro usuário. Talvez os usuários envolvidos nos bugs com classificação importante tenham privilégios mais baixos do que seus colegas com classificação crítica. Abaixo estão listadas as CVEs com classificação crítica:

CVE-2021-28460 / CVE-2021-28480,81,82 e 82 / CVE-2021-28329, 30, 31, 32 ,33 ,34 ,35 ,36 ,37 ,38 ,39 /

CVE-2021-28343 / CVE-2021-27095 / CVE-2021-28315.

- CVE-2021-28444 – Windows Hyper-V Security Feature Bypass Vulnerability

Esse desvio de recurso de segurança permite que um invasor desvie potencialmente as configurações do Router Guard no Hyper-V. O Router Guard foi projetado para impedir que sistemas operacionais convidados ofereçam serviços de roteador na rede. Muitos não percebem que o Windows pode ser configurado como um roteador e, em sistemas físicos ou virtuais, ser configurado para redirecionar pacotes para um local incorreto (por exemplo, Man-in-the-Middle) ou simplesmente criar um buraco negro no tráfego.

É possível que um invasor, uma vez autenticado no servidor Exchange, obtenha acesso ao AD (Active Directory) e assim ter acesso a todo dado contido nele.
O Microsoft Security Intelligence lançou um tweet sobre o ransomware DearCry (O malware criptografa arquivos em um dispositivo e exige resgate em troca de descriptografia) sendo usado para explorar servidores Exchange locais comprometidos. As infecções de ransomware podem ter consequências negativas para uma organização afetada, incluindo:

- Perda temporária ou permanente de informações confidenciais ou proprietárias;
- Interrupção das operações regulares;
- Perdas financeiras incorridas para restaurar sistemas e arquivos;
- Dano potencial à reputação de uma organização.

TÁTICAS, TÉCNICAS E PROCEDIMENTOS

O ransomware tenta criptografar arquivos específicos, identificados pela extensão do arquivo, no sistema de destino utilizando os algoritmos de criptografia Advanced Encryption Standard (AES) e Rivest – Shamir – Adleman (RSA). O ransomware contém a seguinte chave RSA pública codificada, que é utilizada para criptografar os arquivos do usuário do sistema de destino.

2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff

Tags

downloader loader ransomware trojan

Details

Name	2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff
Size	1322496 bytes
Type	PE32 executable (console) Intel 80386, for MS Windows
MD5	0e55ead3b8fd305d9a54f78c7b56741a
SHA1	f7b084e581a8dcea450c2652f8058d93797413c3
SHA256	2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff
SHA512	5c3d58d1001dce6f2d23f33861e9c7fef766b7fe0a86972e9f1eeb70bfad970b02561da6b6d193cf24bc3c1aaf2a42a950fa6e5dff36386653b8aa725c9abaaa
ssdeep	24576:LU5NX2yJOiUXmEICxu2WAP0NIzkQM+KpPRQ9StIUDpl1fpxkHVZgMCS+:L7XP7P9o5QzUtl1fpxkHVZgMC3
Entropy	6.994611

Figura 1: Variante DearCry (Hashs obtidas)

Antivirus

Ahnlab	Ransomware/Win.DoejoCrypt
Antiy	Trojan[Ransom]/Win32.DearCry
Avira	TR/FileCoder.HW
BitDefender	Trojan.GenericKD.36477740
ClamAV	Win.Ransomware.Dearcry-9840778-0
Comodo	Malware
Cyren	W32/Trojan.FOGJ-5046
ESET	a variant of Win32/Filecoder.DearCry.A trojan
Emsisoft	Trojan.GenericKD.36477740 (B)
Ikarus	Trojan-Ransom.FileCrypter
K7	Trojan (005790de1)
Lavasoft	Trojan.GenericKD.36477740
McAfee	Ransom-DearCry!0E55EAD3B8FD
Microsoft Security Essentials	Ransom:Win32/DoejoCrypt.A
NANOAV	Trojan.Win32.Encoder.ipilfs
NetGate	Trojan.Win32.Malware
Quick Heal	Ransom.DearCry.S19261705
Sophos	Troj/Ransom-GFE
Symantec	Downloader
TACHYON	Ransom/W32.DearCry.1322496
TrendMicro	Ransom.56DC2A23
TrendMicro House Call	Ransom.56DC2A23
Vir.IT eXplorer	Ransom.Win32.DearCry.CUQ
VirusBlokAda	TrojanRansom.Encoder
Zillya!	Trojan.Encoder.Win32.2195

Figura 2: identificação por Antivirus

Durante o tempo de execução, o ransomware carrega a chave pública RSA embutida em código. Em seguida, ele tenta identificar todas as unidades que estão conectadas ao sistema conectado, da unidade A: para a unidade Z :. Para cada unidade identificada, o ransomware irá enumerá-la e criptografar arquivos com as seguintes extensões:

.TIF .TIFF .PDF .XLS .XLSX .XLTM .PS .PPS .PPT .PPTX .DOC .DOCX .LOG .MSG .RTF .TEX .TXT .CAD .WPS .EML .INI .CSS .HTM .HTML .XHTML .JS .JSP .PHP .KEYCHAIN .PEM .SQL .APK .APP .BAT .CGI .ASPX .CER .CFM .C .CPP .GO .CONFIG .PL .PY .DWG .XML .JPG .BMP .PNG .EXE .DLL .CAD .AVI .H.CSV .DAT .ISO .PST .PGD .7Z .RAR .ZIP .ZIPX .TAR .PDB .BIN .DB .MDB .MDF .BAK .LOG .EDB .STM .DBF .ORA .GPG .EDB .MFS

Em seguida, o ransomware criptografará os arquivos que tenham as extensões de arquivo listadas acima. Após a criptografia dos arquivos, o ransomware deixará a nota de resgate "readme.txt" dentro de pastas com arquivos criptografados no sistema de destino. nele contém a seguinte mensagem:

If you want to decrypt, please contact us.

konedieyp[@]airmail.cc or uenwonken[@]memail.com

And please send me the following hash!

638428e5021d4ae247b21acf9c0bf6f6

O ransomware irá então excluir a cópia original do arquivo e, em seguida, substituí-los por cópias criptografadas de si mesmo, com a extensão do arquivo alterada para .CRYPT. Antes de realmente excluir o arquivo de destino original, o malware irá sobrescrevê-lo com o valor de repetição 0x41 para tornar impossível a recuperação do arquivo usando o software forense do computador.

Antes de criptografar os arquivos do usuário do sistema de destino, o malware criptografará as informações sobre os arquivos, incluindo o caminho completo do arquivo e a chave AES usada para criptografá-lo, que também será usada para descriptografá-lo. Esses dados serão criptografados usando a chave RSA pública codificada mencionada acima e adicionada ao início do arquivo criptografado. OBS: O ransomware irá gerar uma nova chave AES para cada arquivo.

Durante a execução, o ransomware executa um serviço denominado “msupdate.” Após o processo de criptografia e instalação da nota de resgate, o serviço “msupdate” é removido.

O ransomware irá então excluir a cópia original dos arquivos e, em seguida, substituí-los por cópias criptografadas de si mesmos com a extensão do arquivo alterada para .CRYPT. Antes de realmente excluir o arquivo de destino original, o malware irá sobrescrevê-lo com o valor de repetição 0x41 para tornar impossível a recuperação do arquivo usando o software forense do computador.

Antes de criptografar os arquivos do usuário do sistema de destino, o malware criptografará as informações sobre os arquivos, incluindo o caminho completo do arquivo e a chave AES usada para criptografá-lo, que também será usada para descriptografá-lo. Esses dados serão criptografados usando a chave RSA pública codificada mencionada acima e adicionada ao início do arquivo criptografado. Nota: O ransomware irá gerar uma nova chave AES para cada arquivo.

RECOMENDAÇÕES PARA TRATATIVA DO DEARCRY

Recomenda-se que os usuários e administradores considerem o uso das práticas recomendadas a seguir para fortalecer a postura de segurança dos sistemas de suas organizações. Todas as alterações de configuração devem ser revisadas pelos proprietários e administradores do sistema antes da implementação para evitar impactos indesejados.

- Mantenha assinaturas e mecanismos de antivírus atualizados;
- Mantenha os patches do sistema operacional atualizados;
- Desative os serviços de compartilhamento de arquivos e impressoras. Se esses serviços forem necessários, use senhas fortes ou autenticação do Active Directory;
- Restrinja a capacidade (permissões) dos usuários de instalar e executar aplicativos de software indesejados. Não adicione usuários ao grupo de administradores locais, a menos que seja necessário;
- Aplique uma política de senha forte e implemente alterações regulares de senha;
- Tenha cuidado ao abrir anexos de e-mail, mesmo que o anexo seja esperado e o remetente pareça ser conhecido;
- Habilite um firewall pessoal nas estações de trabalho, configurado para negar solicitações de conexão não solicitadas;
- Desative serviços desnecessários em estações de trabalho e servidores;

- Procure e remova anexos de e-mail suspeitos; certifique-se de que o anexo verificado é seu "tipo de arquivo verdadeiro" (ou seja, a extensão corresponde ao cabeçalho do arquivo);
- Monitore os hábitos de navegação dos usuários na web; restringir o acesso a sites com conteúdo desfavorável;
- Tenha cuidado ao usar mídia removível (por exemplo, pen drives USB, drives externos, CDs, etc.);
- Faça a varredura de todo o software baixado da Internet antes de executá-lo;
- Mantenha a consciência situacional das ameaças mais recentes e implemente Listas de Controle de Acesso (ACLs) apropriadas.

AINDA SOBRE VULNERABILIDADES

Identificação de 10 webshells

Identificou-se aproximadamente 10 webshells associadas a atividade do ransonware. Esta não é uma lista completa de webshells que estão sendo aproveitadas pelos atores. Recomenda-se que as organizações revisem os MARs a seguir para uma análise detalhada dos 10 webshells, junto com TTPs e IOCs. Esses MARs incluem regras YARA desenvolvidas para ajudar na detecção e resposta em tempo hábil.

1. AR21-072A: MAR-10328877.r1.v1: China Chopper Webshell
2. AR21-072B: MAR-10328923.r1.v1: China Chopper Webshell
3. AR21-072C: MAR-10329107.r1.v1: China Chopper Webshell
4. AR21-072D: MAR-10329297.r1.v1: China Chopper Webshell
5. AR21-072E: MAR-10329298.r1.v1: China Chopper Webshell
6. AR21-072F: MAR-10329301.r1.v1: China Chopper Webshell
7. AR21-072G: MAR-10329494.r1.v1: China Chopper Webshell
8. AR21-084A: MAR-10329496-1.v1: China Chopper Webshell
9. AR21-084B: MAR-10329499-1.v1: China Chopper Webshell
10. AR21-102A: MAR-10331466-1.v1: China Chopper Webshell
11.

Um webshell é um script que pode ser carregado em um Microsoft Exchange Server comprometido para permitir a administração remota da máquina. Webshells são utilizados para os seguintes fins:

- Coletar e filtrar dados e credenciais confidenciais;

- Fazer upload de malware adicional com o potencial de criar, por exemplo, um watering hole (utilidade do Botnet) para infecção e varredura de outras vítimas;
- Usar como um ponto de retransmissão para emitir comandos para hosts dentro da rede sem acesso direto à Internet;
- Para usar como infraestrutura de comando e controle, potencialmente na forma de um bot em um botnet ou no suporte de comprometimento de redes externas adicionais. Isso pode ocorrer se o adversário pretende manter a persistência de longo prazo. Geralmente conhecido como DDos (Ataque de negação de serviço).

Foi observado os seguintes arquivos como alvos de solicitações HTTP POST:

- /owa/auth/Current/themes/resources/logon.css
- /owa/auth/Current/themes/resources/owafont_ja.css
- /owa/auth/Current/themes/resources/lgnbotl.gif
- /owa/auth/Current/themes/resources/owafont_ko.css
- /owa/auth/Current/themes/resources/SegoeUI-SemiBold.eot
- /owa/auth/Current/themes/resources/SegoeUI-SemiLight.ttf
- /owa/auth/Current/themes/resources/lgnbotl.gif

Os administradores devem pesquisar os logs do servidor ECP para a seguinte string (ou algo semelhante):

S:CMD=Set-OabVirtualDirectory.ExternalUrl='

Os logs podem ser encontrados em <exchange install path>\Logging\ECP\Server\.

Para determinar a possível atividade do webshell, os administradores devem pesquisar arquivos aspx nos seguintes caminhos:

- \inetpub\wwwroot\aspnet_client\ (qualquer arquivo aspx nesta pasta ou subpastas)
- \<exchange install path>\FrontEnd\HttpProxy\ecp\auth\ (qualquer arquivo além TimeoutLogoff.aspx)
- \<exchange install path>\FrontEnd\HttpProxy\owa\auth\ (qualquer arquivo ou arquivo modificado que não faça parte de uma instalação padrão)

- \<exchange install path>\FrontEnd\HttpProxy\owa\auth\Current\ (qualquer aspx arquivo nesta pasta ou subpastas)
- \<exchange install path>\FrontEnd\HttpProxy\owa\auth\<folder with version number>\ (qualquer arquivo aspx nesta pasta ou subpastas)

Também pesquisar sobre /owa/auth/Current os seguintes agentes de usuário de log da web fora do padrão. Esses agentes podem ser úteis para os responsáveis pela resposta a incidentes determinar se uma investigação mais aprofundada é necessária.
Estes não devem ser considerados como IOCs definitivos:

- DuckDuckBot/1.0;+(+http://duckduckgo.com/duckduckbot.html)
- facebookexternalhit/1.1+(+http://www.facebook.com/externalhit_uatext.php)
- Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www.baidu.com/search/spider.html)
- Mozilla/5.0+(compatible;+Bingbot/2.0;++http://www.bing.com/bingbot.htm)
- Mozilla/5.0+(compatible;+Googlebot/2.1;++http://www.google.com/bot.html
- Mozilla/5.0+(compatible;+Konqueror/3.5;+Linux)+KHTML/3.5.5+(like+Gecko)+(Exabot-Thumbnails)
- Mozilla/5.0+(compatible;+Yahoo!+Slurp;+http://help.yahoo.com/help/us/ysearch/slurp)
- Mozilla/5.0+(compatible;+YandexBot/3.0;++http://yandex.com/bots)
- Mozilla/5.0+(X11;+Linux+x86_64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/51.0.2704.103+Safari/537.36

Foi observado também, agentes de usuário em conjunto com a exploração de URLs /ecp/:

- ExchangeServicesClient/0.0.0.0
- python-requests/2.19.1
- python-requests/2.25.1

Esses agentes também foram observados tendo conexões para acesso pós-exploração do shell da web:

- antSword/v2.1
- Googlebot/2.1+(+http://www.googlebot.com/bot.html)
- Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www.baidu.com/search/spider.html)

Assim como acontece com os agentes de usuário não padrão, os respondentes podem examinar os logs dos serviços de informações da Internet (IIS) dos servidores Exchange para identificar possíveis atividades históricas. Além disso, como acontece com os agentes de usuário não padrão, eles não devem ser considerados como IOCs definitivos:

- POST /owa/auth/Current/
- POST /ecp/default.flt
- POST /ecp/main.css
- POST /ecp/<single char>.js

Os seguintes endereços IP foram utilizados pelos agentes maliciosos. Embora estes estejam ligados a servidores virtuais privados (VPSs) e redes virtuais privadas (VPNs), os respondentes devem investigar esses endereços IP em suas redes e agir conforme suas políticas internas:

- 103.77.192[.]219
- 104.140.114[.]110
- 104.250.191[.]110
- 108.61.246[.]56
- 149.28.14[.]163
- 157.230.221[.]198
- 167.99.168[.]251
- 185.250.151[.]72
- 192.81.208[.]169
- 203.160.69[.]66
- 211.56.98[.]146
- 5.254.43[.]18
- 5.2.69[.]14

- 80.92.205[.]81
- 91.192.103[.]43

São apresentados abaixo os hashes de webshell fornecidos pela Microsoft:

- b75f163ca9b9240bf4b37ad92bc7556b40a17e27c2b8ed5c8991385fe07d17d0
- 097549cf7d0f76f0d99edf8b2d91c60977fd6a96e4b8c3c94b0b1733dc026d3e
- 2b6f1ebb2208e93ade4a6424555d6a8341fd6d9f60c25e44afe11008f5c1aad1
- 65149e036fff06026d80ac9ad4d156332822dc93142cf1a122b1841ec8de34b5
- 511df0e2df9bfa5521b588cc4bb5f8c5a321801b803394ebc493db1ef3c78fa1
- 4edc7770464a14f54d17f36dc9d0fe854f68b346b27b35a6f5839adf1f13f8ea
- 811157f9c7003ba8d17b45eb3cf09bef2cecd2701cedb675274949296a6a183d
- 1631a90eb5395c4e19c7dbcbf611bbe6444ff312eb7937e286e4637cb9e72944

Observação: esta não é uma lista completa de indicadores de comprometimento e os agentes de ameaça costumam usar endereços IP alugados de curto prazo que mudam com muita frequência. As organizações que não localizam nenhum dos IOCs neste Alerta em seu tráfego de rede podem ter sido comprometidas. Recomendamos que seu profissional especialista em Microsoft Exchange siga as orientações sugerida pela [Microsoft].

MITIGAÇÃO

De acordo com a Microsoft, a empresa está ciente dos agentes de ameaças que usam ferramentas de código aberto para pesquisar servidores Microsoft Exchange vulneráveis. Esse tipo específico de ataque pode ser feito por script, permitindo que os invasores explorem vulnerabilidades por meio de mecanismos automatizados.

Verifique as atualizações de segurança estão disponíveis para os seguintes sistemas operacionais:

- Exchange Server 2010 (a atualização requer SP3 ou qualquer SP3RU)
- Exchange Server 2013 (atualização requer CU 23)
- Exchange Server 2016 (a atualização requer CU 19 ou CU 18)
- Exchange Server 2019 (a atualização requer CU 8 ou CU 7)

Todos os patches devem ser aplicados usando privilégios de administrador.
Se a correção não for uma opção imediata, recomenda-se uma solução temporária, não como um substituto para o patch. Além disso, existem outras opções de mitigação disponíveis. Recomenda-se limitar ou bloquear o acesso externo a servidores Exchange voltados para a Internet por meio do seguinte:

- Restrinja conexões não confiáveis à porta 443 ou configure uma VPN para separar o Exchange Server do acesso externo; observe que isso não impedirá que um adversário explore a vulnerabilidade se o invasor já estiver em sua rede;
- Bloqueie o acesso externo ao Exchange local;
- Restringir o acesso externo ao OWA URL: /owa/;
- Restringir o acesso externo para o Exchange Admin Center (EAC) aka Painel de Controle do Exchange (ECP) URL: /ecp/;
- Desconecte servidores Exchange vulneráveis da Internet até que um patch possa ser aplicado;
- Investigue servidores Exchange expostos para comprometimento, independentemente do status do patch atual;
- Procure por shells da web por meio de nossa orientação e execute uma verificação AV completa usando a ferramenta de mitigação do Exchange no local;
- Investigue usuários e grupos locais, até mesmo usuários não administrativos, para alterações e certifique-se de que todos os usuários exijam uma senha para entrar. As criações de novas contas de usuário (representadas pela ID de evento 4720) durante o tempo em que o sistema estava vulnerável podem indicar a criação de um usuário mal-intencionado;
- Redefina e randomize as senhas do administrador local com uma ferramenta como LAPS, se ainda não estiver fazendo isso;
- Procure alterações na configuração de RDP, firewall, assinaturas WMI e Gerenciamento Remoto do Windows (WinRM) do sistema que podem ter sido configuradas pelo invasor para permitir persistência;
- Procure a ID de evento 1102 para determinar se os invasores limparam os logs de eventos, uma atividade que os invasores executam com exe na tentativa de ocultar seus rastros;

- Procure novos mecanismos de persistência, como serviços inesperados, tarefas agendadas e itens de inicialização;
- Procure ferramentas Shadow IT que os invasores possam ter instalado para persistência, como RDP não Microsoft e clientes de acesso remoto;
- Verifique as configurações de encaminhamento de email no nível da caixa de correio (atributos ForwardingAddress e ForwardingSMTPAddress), verifique as regras da caixa de entrada da caixa de correio (que podem ser usadas para encaminhar email externamente) e verifique as regras de Transporte do Exchange que você pode não reconhecer.

Fontes

- Microsoft's April 2021 Security Update that mitigates significant vulnerabilities affecting on-premises Exchange Server 2016 and 2019.
- Microsoft Advisory: https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/
- Microsoft Security Blog - Hafnium targeting Exchange Servers: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
- Volexity Blog: https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/
- Microsoft's blog on Exchange Server Vulnerabilities Mitigations: https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/

Referências

Eric Zimmerman: KAPE Documentation

Emergency Directive 21-02: Mitigate Microsoft Exchange On-Premises Product Vuln...

Supplemental Direction V1 to Emergency Directive 21-02: Mitigate Microsoft Exch...

Supplemental Direction V2 to Emergency Directive 21-02: Mitigate Microsoft Exch...

https://us-cert.cisa.gov/ncas/analysis-reports/ar21-102b