heimdall

security research

A DIVISION OF ISH

heimdall
security research

Principais vulnerabilidades exploradas em ataques cibernéticos em 2022

Sumário

1 O QUE É VULNERABILIDADE?

Para a área da segurança cibernética, podemos afirmar que a vulnerabilidade é uma fraqueza que pode ser explorada por criminosos cibernéticos para obter acesso não autorizado a um sistema. Após essa exploração, o criminoso cibernético pode executar códigos maliciosos e *malware*s e até mesmo realizar exfiltração de dados.

Vale salientar que diversos *software*s populares podem possuir vulnerabilidades, sendo estas classificadas de acordo com a sua criticidade e como grande ou baixo risco de serem exploradas.

Quanto às vulnerabilidades de segurança cibernéticas divulgadas publicamente, existe o programa CVE, um registro para cada vulnerabilidade no catálogo, que as identifica, define e cataloga.

Com isto, antes de serem publicadas por organizações de todo o mundo, é atribuído um ID a cada vulnerabilidade. Assim, ao serem discutidas e compartilhadas informações sobre as vulnerabilidades haverá um ID vinculado.

Diante disto, a **ISH Tecnologia** realizou pesquisas e reuniu as **principais vulnerabilidades exploradas em 2022**, bem como as **principais vulnerabilidades exploradas por famílias/grupos de *Ransomware* em 2022**.

2 CVEs CONSUMIDAS PELO GTI

Abaixo, ilustramos a quantidade de CVEs tratados diariamente pelo **GTI**, trazendo diversas vulnerabilidades nas quais o ambiente conectado junto ao GTI pode receber de forma constante o referido alerta.

2.1 CVEs IDENTIFICADAS NO GTI

A ISH Tecnologia, por meio do GTI, realiza a pesquisa e monitoramento dos principais CVEs publicadas que visam atingir todos os tipos de ambientes e dispositivos, reunindo-os e gerando alertas diários de tais vulnerabilidades, incluindo as recém-publicadas.

Abaixo listamos as vulnerabilidades identificadas nos últimos 90 (noventa) dias, classificando-as de acordo com a sua criticidade (crítica, alta, média e baixa).

Figura 1 – Indicadores relacionadas às vulnerabilidades identificadas em 90 dias de acordo com GTI.

Além disso, o GTI realiza a descrição da vulnerabilidade e do ativo que está em risco de ser alvo ou que foi afetado pela vulnerabilidade, apresentando, conforme a imagem abaixo, a descrição, vulnerabilidade, severidade, *score* e *data*, e outros dados que se tornam relevantes para o alerta.

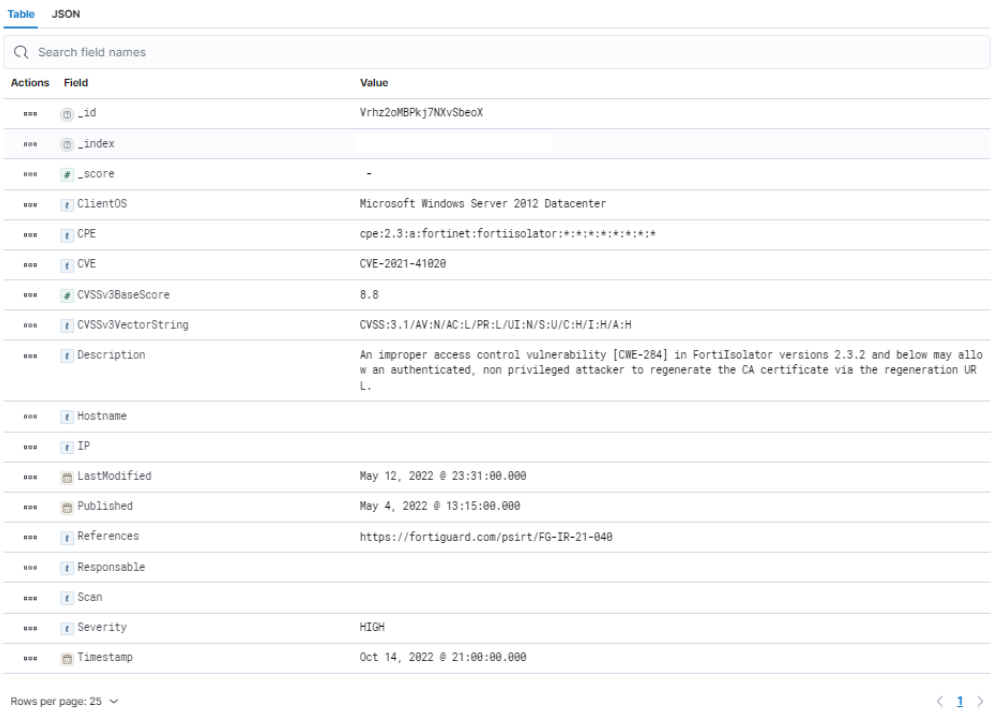

Table JSON

Search field names

Actions	Field	Value
	_id	VrhZ2oMBPkj7NXvSbeoX
	_index	
	_score	-
	ClientOS	Microsoft Windows Server 2012 Datacenter
	CPE	cpe:2.3:a:fortinet:fortiisolator:*:*:*:*:*:*:*:*
	CVE	CVE-2021-41020
	CVSSv3BaseScore	8.8
	CVSSv3VectorString	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
	Description	An improper access control vulnerability [CWE-284] in FortiIsolator versions 2.3.2 and below may allow an authenticated, non privileged attacker to regenerate the CA certificate via the regeneration URL.
	Hostname	
	IP	
	LastModified	May 12, 2022 @ 23:31:00.000
	Published	May 4, 2022 @ 13:15:00.000
	References	https://fortiguard.com/psirt/FG-IR-21-040
	Responsable	
	Scan	
	Severity	HIGH
	Timestamp	Oct 14, 2022 @ 21:00:00.000

Rows per page: 25 1

Figura 2 – Descrição da vulnerabilidade localizada no host de acordo com o GTI, informando severidade, referências, IP, descrição e CVE.

Diante disto, a ISH Tecnologia entrega em momento ideal as vulnerabilidades recém-publicadas e divulgadas, visando garantir a proteção do ambiente da organização.

3 VULNERABILIDADES MAIS EXPLORADAS EM 2022

A **ISH Tecnologia**, por meio do time de **Threat Intelligence Heimdall**, apresenta as principais vulnerabilidades exploradas e importantes no ano de 2022 que foram coletadas em fontes abertas, sendo que não estão necessariamente classificadas com base em ataques identificados, mas sim na severidade da vulnerabilidade identificada.

3.1 PROXY*LOGON* (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065)

Proxy*Logon* é uma vulnerabilidade identificada que afeta o Microsoft Exchange 2013, 2016 e 2019. Ela permite que um adversário ignore a autenticação e, assim, se passe por um administrador. Devido à falta de atualizações da infraestrutura interna, continua sendo uma das vulnerabilidades mais exploradas em 2022.

Vale salientar que esta vulnerabilidade foi publicada em agosto de 2021 pela equipe DEVCORE, sendo adicionada a vários kits de ferramentas automáticas e usada por uma ampla gama de agentes de ameaças para empregar códigos maliciosos. Esta falha pode ser explorada na porta 433 sem interação do usuário, auxiliando os criminosos cibernéticos em movimentação lateral acesso persistente e manipulação remota.

3.2 ZERO*LOGON* (CVE-2020-1472)

O CVE-2020-1472, conhecido como Zero*Logon*, apesar de ter sido publicada e conhecida a partir de agosto de 2020, ainda continua a ser explorada pelos criminosos cibernéticos. Essa vulnerabilidade reside em uma falha criptográfica no processo de *login*, sendo que, ao ser aproveitada, um adversário pode se conectar com o protocolo remoto de *logon* de rede do diretório ativo (MS-NRPC) e fazer *logon* usando NTLM.

A Microsoft publicou, em novembro de 2020, que a Zero*Logon* seria detectada pelo Microsoft Defender, afirmando ainda que a referida vulnerabilidade poderia ocasionar a escalação de privilégio de *logon* de rede.

3.3 LOG4SHELL (CVE-2021-44228)

A vulnerabilidade conhecida como Log4Shell, publicada em dezembro de 2021, ainda se encontra em evidência em 2022, pois essa vulnerabilidade afeta a biblioteca de *log* Apache Java, conhecida como Log4j. A referida biblioteca é utilizada por muitas aplicações da *Web* e por isto os criminosos cibernéticos aproveitaram e aproveitam constantemente.

Esta vulnerabilidade pode ser testada e explorada a partir de qualquer ponto de entrada em que o usuário externo tenha permissão para inserir dados. Os pontos de entrada são: formulários de *login* e senha, cabeçalhos HTTP como User-Agent, X-*Forwarded-For* e outros cabeçalhos personalizados.

3.4 VMware vSphere client (CVE-2021-21972)

A vulnerabilidade de execução remota de código é classificada com a taxa de gravidade de 9,8 e foi descoberta em fevereiro de 2021 no VMware cSphere cliente (HTML5). Lembrando que o vSphere é um virtualizador popular usado por organizações.

O criminoso cibernético, ao explorá-la, pode escalar privilégios e executar comandos remotos na porta 443 por meio da vulnerabilidade. Após isto, a máquina pode ser utilizada como "trampolim" para acessar toda a infraestrutura da organização.

A VMware publicou detalhes sobre a referida vulnerabilidade em um relatório, inclusive a sua correção para atualizações do produto.

3.5 PetitPotam (CVE-2021-36942)

A vulnerabilidade PetitPotam está presente em servidores Windows, onde os serviços de certificados do Active Directory (AD CS) não estão configurados com proteção contra-ataques de retransmissão NTLM. Um criminoso cibernético pode assumir o controle de um controlador de domínio, forçando-o a se autenticar em um servidor de retransmissão NTML controlado pelo mesmo e, em seguida, realiza a interceptação do tráfego e personifica os clientes.

Esta vulnerabilidade pode ser corrigida instalando o KB5005413 ou garantindo que os serviços que permitem a autenticação NTLM utilizem métodos de segurança, como a proteção estendida para autenticação ou recursos de assinaturas.

3.6 Zoho ManageEngine ADSelfService Plus (CVE-2021-40539)

O Zoho ManageEngine ADselfService Plus, antes de incluir a versão 6113, foi considerado vulnerável a um desvio de autenticação da API REST e subsequente execução remota de código. A vulnerabilidade permite que os invasores usem URLs da API Rest especialmente criados para ignorar a autenticação devido a um erro na normalização do URL antes de tentar a validação. Tendo contornado o filtro de autenticação, os invasores podem explorar *endpoints* e realizar ataques como a execução arbitrária de comandos.

Para fins de obtenção de maiores informações da vulnerabilidade e mitigação, recomendamos que seja acessado o Comunicado de Segurança sobre vulnerabilidade.

3.7 ProxyShell (CVE-2021-31207, CVE-2021-34473 e CVE-2021-34523)

A vulnerabilidade conhecida como ProxyShell consiste em três falhas separadas no servidor de e-mail do Microsoft Exchange, permitindo o desvio de recursos de segurança, RCE e elevação de privilégio. Quando utilizada em ambientes expostos, o ProxyShell permite que um criminoso cibernético estabeleça persistência e execute comandos maliciosos do PowerShell. Esta exploração, caso bem-sucedida, permite que os criminosos assumam o controle total dos servidores de e-mail Microsoft Exchange vulneráveis.

Essas vulnerabilidades foram identificadas pela primeira vez em agosto de 2021, no *Microsoft Client Access Service* (CAS), um serviço que normalmente é executado na porta 443 no *Microsoft Internet Information Services* (IIS) e é comumente exposto à Internet para que os usuários possam acessar e-mails de dispositivos móveis e navegadores da *web*.

3.8 Atlassian Confluence Server & Data Center (CVE-2021-26084)

A CVE-2021-26084 é uma vulnerabilidade de segurança de gravidade crítica que permite que um usuário não autenticado execute um código arbitrário em uma instância do *Confluence Server* ou *Data Center*. O *Confluence* é um serviço de estilo *Wiki* amplamente implantado em organizações. A referida vulnerabilidade foi divulgada em agosto de 2021, sendo que continua sendo explorada ativamente.

Para obter mais detalhes e mitigação, recomendamos que seja consultada a comunicação da *Confluence*.

3.9 Pulse Secure Pulse Connect Secure (CVE-2019-11510)

A CVE-2019-11510 é uma vulnerabilidade que afeta os dispositivos Pulse Secure VPN, que permite que os criminosos cibernéticos obtenham acesso às redes das vítimas. Um invasor remoto não autenticado pode enviar um URI especialmente criado para executar uma vulnerabilidade de leitura arbitrária de arquivo.

Os *patches* de correção foram lançados em abril de 2019, porém, vários incidentes ocorreram em que credenciais de AD comprometidas foram usadas meses depois que organizações vítimas corrigiram seu dispositivo VPN.

3.10 Fortinet FortiOS e FortiProxy (CVE-2018-13379)

A CVE-2018-13379 é uma vulnerabilidade no portal da *web* FortiProxy SSL VPN. Na exploração, a vulnerabilidade pode permitir que um invasor remoto não autenticado baixe arquivos do sistema FortiProxy por meio de solicitações de recursos HTTP criadas.

Para obter mais detalhes sobre essa vulnerabilidade e mitigação, recomendamos consultar o comunicado da Fortiguard referente a tal vulnerabilidade.

3.11 FOLINA (CVE-2022-30190)

A CVE-2022-30190 é uma vulnerabilidade que permite a execução remota de código quando o MSDT é chamado usando o protocolo de URL de um aplicativo de chamada, como o *Word*. O criminoso cibernético pode explorar com êxito essa vulnerabilidade e poderá executar código arbitrário com os privilégios do aplicativo de chamada.

Para obter mais detalhes sobre a vulnerabilidade e mitigação, recomendamos consultar o comunicado da Microsoft referente a referida vulnerabilidade.

3.12 SPRING4SHELL (CVE-2022-22965)

A CVE-2022-22965 trata que um aplicativo *Spring* MVC ou *Spring WebFlux* em execução no JDK 9+ pode ser vulnerável à execução remota de código por meio de vinculação de dados. A exploração específica requer que o aplicativo seja executado no Tomcat como uma implantação WAR.

Para obter mais detalhes sobre a vulnerabilidade e mitigação, recomendamos consultar o comunicado da CVE referente a tal vulnerabilidade.

3.13 F5 BIG-IP (CVE-2022-1388)

A CVE-2022-1388 pode permitir que um invasor não autenticado com acesso de rede ao sistema BIG-IP por meio da porta de gerenciamento e/ou endereços IP próprios execute comandos arbitrários do sistema, crie ou exclua arquivos ou desabilite serviços.

Para obter mais detalhes sobre a vulnerabilidade e mitigação, recomendamos consultar o comunicado da F5 referente a tal vulnerabilidade.

3.14 GOOGLE CHROME (CVE-2022-0609)

A CVE-2022-0609 permitia que um invasor remoto explorasse potencialmente a corrupção de *heap* por meio de uma página HTML criada, sendo que a vulnerabilidade atingia as versões anteriores a 98.0.4758.102.

Para obter mais detalhes sobre a vulnerabilidade e mitigação, recomendamos consultar o comunicado da Google referente a tal vulnerabilidade.

3.15 ZIMBRA COLLABORATION SUITE BUGS (CVE-2022-27925 E CVE-2022-41352)

A CVE-2022-27925 nas versões do Zimba Collaboration 8.8.15 e 9.0 possui funcionalidades *mboximport* que recebe um arquivo ZIP e extrai arquivos dele. Um usuário autenticado com direitos de administrador tem a capacidade de fazer upload de arquivos arbitrários para o sistema, levando à travessia do diretório.

Já a CVE-2022-41352, permite que um invasor realize upload de arquivos arbitrários por meio do amavisd por meio de uma brecha cpio que pode levar ao acesso incorreto a qualquer outra conta de usuário.

Para obter mais detalhes sobre a vulnerabilidade e mitigação, recomendamos consultar o comunicado da Zimbra referente a tal vulnerabilidade.

Apesar de todas as vulnerabilidades descritas acima, o time de **Threat Intelligence Heimdall** apresenta ainda as principais vulnerabilidades críticas utilizadas por grupos/famílias de *Ransomware* em 2022.

4 *RANSOMWARE* MAIS ATIVOS EM 2022

De acordo com o monitoramento contínuo de divulgação através de canais de *Data Leaks*, a ***Darkfeed*** compilou e categorizou os principais grupos ativos até o momento, obtendo o resultado abaixo:

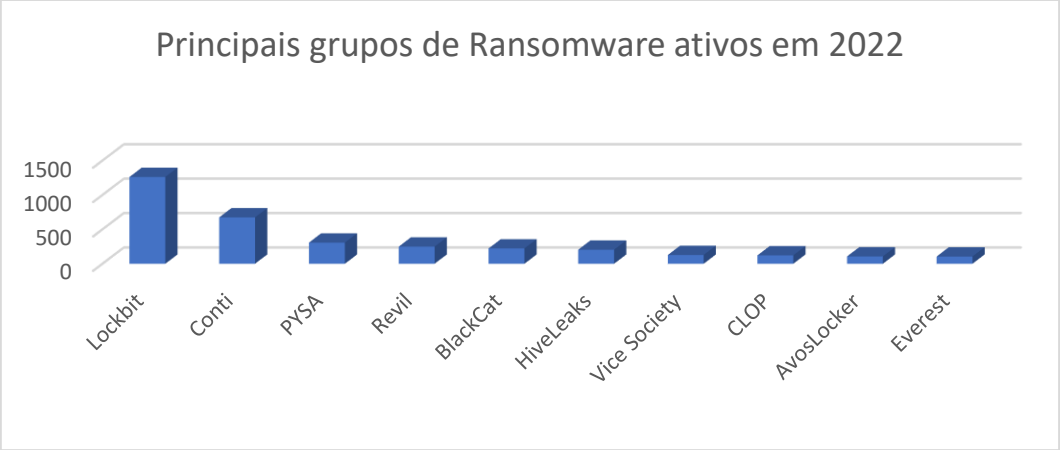

Gráfico 1 – Principais grupos relacionados a Ransomwares de acordo com o Darkfeed, consultado em 08/12/2022.

Legenda:	
Grupo/Família	**Quant.**
Lockbit	1261
Conti	674
PYSA	307
Revil	249
BlackCat	222
HiveLeaks	204
Vice Society	127
CLOP	122
AvosLocker	106
Everest	105

Foram ainda contabilizados, por meio de pesquisa de fontes abertas, **4.323** (quatro mil trezentos e vinte e três) postagens relacionadas a vazamento de dados somente no ano de 2022.

Ainda, o especialista e membro do CSIRT da Recorded Future, Allan Liska, acabou por divulgar e compilar uma lista das vulnerabilidades exploradas pelas famílias de *ransomware*.

Abaixo, compartilhamos de forma esquemática as principais vulnerabilidades exploradas:

Figura 3 - As vulnerabilidades mais exploradas por Ransomwares

5 DESCRIÇÃO DAS VULNERABILIDADES

Abaixo listamos os principais aspectos de cada vulnerabilidade compartilhada acima. Para acessar a vulnerabilidade basta clicar sobre a CVE para o encaminhamento ao site do Mitre.

5.1 PULSESECUREVPN:

CVE-2021-22893	O Pulse Connect Secure 9.0R3/9.1 (e superior) é vulnerável a um desvio de autenticação exposto pelo *Windows File Share Browser* e pelos recursos *Pulse Secure Collaboration* do Pulse Connect Secure que podem permitir que um usuário não autenticado realize a execução remota de código arbitrário no Pulse Connect Secure.
CVE-2020-8260	Uma vulnerabilidade na interface da *Web* do administrador do Pulse Connect Secure < 9.1R9 que pode permitir que um invasor autenticado realize uma execução arbitrária de código usando extração gzip.
CVE-2020-8243	Vulnerabilidade na interface da *Web* do administrador do Pulse Connect Secure < 9.1R8.2 que pode permitir que um invasor autenticado carregue um modelo personalizado para executar código arbitrário.
CVE-2019-11539	No Pulse Secure Pulse Connect Secure versão 9.0RX anterior a 9.0R3.4, 8.3RX anterior a 8.3R7.1, 8.2RX anterior a 8.2R12.1 e 8.1RX anterior a 8.1R15.1 e Pulse Policy Secure versão 9.0RX anterior a 9.0R3. 2, 5.4RX anterior a 5.4R7.1, 5.3RX anterior a 5.3R12.1, 5.2RX anterior a 5.2R12.1 e 5.1RX anterior a 5.1R15.1, na qual a interface *web* de administração permite que um invasor autenticado injete e execute comandos.
CVE-2019-11510	No Pulse Secure Pulse Connect Secure (PCS) 8.2 anterior a 8.2R12.1, 8.3 anterior a 8.3R7.1 e 9.0 anterior a 9.0R3.4, um agente remoto não autenticado pode enviar em URI especialmente criado para executar uma vulnerabilidade de leitura de arquivo arbitrária.

5.2 CITRIX:

CVE-2020-8196	Controle de acesso impróprio nas versões Citrix ADC e Citrix Gateway anteriores a 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 e 10.5-70.18 e versões Citrix SDWAN WAN-OP anteriores a 11.1.1a, 11.0.3d e 10.2.7, resultando na divulgação limitada de informações para usuários com poucos privilégios.
CVE-2020-8195	Validação de entrada inadequada nas versões *Citrix ADC* e *Citrix Gateway* anteriores a 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 e 10.5-70.18 e versões Citrix SDWAN WAN-OP anteriores a 11.1.1a, 11.0.3d e 10.2.7 resultantes na divulgação limitada de informações para usuários com poucos privilégios.
CVE-2019-19781	Foi descoberto um problema no *Citrix Application Delivery Controller* (ADC) e no *Gateway* 10.5, 11.1, 12.0, 12.1 e 13.0. Eles permitem *Directory Traversal.*
CVE-2019-11634	O *Citrix Workspace App* antes de 1904 para Windows tem controle de acesso incorreto.
CVE-2021-22941	Controle de acesso impróprio no controlador de zonas de armazenamento *Citrix ShareFile* antes de 5.11.20 pode permitir que um invasor não autenticado comprometa remotamente o controlador de zonas de armazenamento.

5.3 MICROSOFT EXCHANGE:

CVE-2021-34523	Vulnerabilidade de elevação de privilégio do *Microsoft Exchange Server* Este ID CVE é exclusivo de CVE-2021-33768, CVE-2021-34470.
CVE-2021-34473	Vulnerabilidade de execução remota de código do *Microsoft Exchange Server.* Este ID CVE é exclusivo de CVE-2021-31196, CVE-2021-31206.
CVE-2021-31207	Vulnerabilidade de desvio do recurso (*bypass*) de segurança do *Microsoft Exchange Server.*
CVE-2021-26855	Vulnerabilidade de execução remota de código do *Microsoft Exchange Server.* Este ID CVE é exclusivo de CVE-2021-26412, CVE-2021-26854, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078.

5.4 FORTINET:

CVE-2020-12812	Uma vulnerabilidade de autenticação imprópria no SSL VPN no FortiOS 6.4.0, 6.2.0 a 6.2.3, 6.0.9 e abaixo pode resultar em um usuário sendo capaz de efetuar *login* com sucesso sem solicitar o segundo fator de autenticação (FortiToken), caso haja mudança de nome de usuário.
CVE-2019-5591	Uma vulnerabilidade de configuração padrão no FortiOS pode permitir que um invasor não autenticado na mesma sub-rede intercepte informações confidenciais representando o servidor LDAP.
CVE-2018-13379	Uma limitação imprópria de um nome de caminho para um diretório restrito ("*Path Traversal*") no Fortinet FortiOS 6.0.0 a 6.0.4, 5.6.3 a 5.6.7 e 5.4.6 a 5.4.12 e FortiProxy 2.0.0, 1.2. 0 a 1.2.8, 1.1.0 a 1.1.6, 1.0.0 a 1.0.7 sob SSL VPN. O portal da *Web* permite que um invasor não autenticado baixe arquivos do sistema por meio de solicitações de recursos HTTP especialmente criados.

5.5 SONICWALL:

CVE-2021-20016	Uma vulnerabilidade SQL-*Injection* no produto SonicWall SSLVPN SMA100 permite que um invasor remoto não autenticado execute uma consulta SQL para acessar a senha do nome de usuário e outras informações relacionadas à sessão. Esta vulnerabilidade afeta o SMA100 *build* versão 10.x.
CVE-2020-5135	Uma vulnerabilidade de *buffer overflow* no SonicOS permite que um invasor remoto cause negação de serviço (DoS) e potencialmente execute código arbitrário enviando uma solicitação maliciosa ao firewall. Esta vulnerabilidade afetou SonicOS Gen 6 versão 6.5.4.7, 6.5.1.12, 6.0.5.3, SonicOSv 6.5.4.v e Gen 7 versão 7.0.0.0.
CVE-2019-7481	A vulnerabilidade no SonicWall SMA100 permite que usuários não autenticados obtenham acesso somente leitura a recursos não autorizados. Essa vulnerabilidade afetou o SMA100 versão 9.0.0.3 e anteriores.

5.6 F5:

CVE-2021-22986	Nas versões BIG-IP 16.0.x anteriores a 16.0.1.1, 15.1.x anteriores a 15.1.2.1, 14.1.x anteriores a 14.1.4, 13.1.x anteriores a 13.1.3.6 e 12.1.x anteriores a 12.1.5.3 amd BIG-IQ 7.1 .0.x antes de 7.1.0.3 e 7.0.0.x antes de 7.0.0.2, a *interface iControl REST* tem uma vulnerabilidade de execução de comando remoto não autenticada.
CVE-2020-5902	Nas versões BIG-IP 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1 e 11.6.1-11.6.5.1, o usuário de gerenciamento de tráfego *Interface* (TMUI), também conhecida como utilitário de configuração, possui uma vulnerabilidade de execução remota de código (RCE) em páginas não divulgadas.

5.7 PALO ALTO:

CVE-2020-2021	Quando a autenticação *Security Assertion Markup Language* (SAML) está habilitada e a opção *'Validate Identity Provider Certificate'* está desabilitada (desmarcada), a verificação imprópria de assinaturas na autenticação PAN-OS SAML permite que um invasor baseado em rede não autenticado acesse recursos protegidos. O invasor deve ter acesso à rede do servidor vulnerável para explorar esta vulnerabilidade. Esse problema afeta as versões do PAN-OS 9.1 anteriores ao PAN-OS 9.1.3; Versões do PAN-OS 9.0 anteriores ao PAN-OS 9.0.9; Versões do PAN-OS 8.1 anteriores ao PAN-OS 8.1.15 e todas as versões do PAN-OS 8.0 (EOL). Esse problema não afeta o PAN-OS 7.1. Esse problema não pode ser explorado se o SAML não for usado para autenticação. Esse problema não pode ser explorado se a opção 'Validar certificado do provedor de identidade' estiver habilitada (marcada) no perfil do servidor do provedor de identidade SAML. Os recursos que podem ser protegidos pela autenticação de *logon* único (SSO) baseada em SAML são*: GlobalProtect Gateway, GlobalProtect Portal, GlobalProtect Clientless VPN, Authentication and Captive Portal, firewalls* PAN-OS de próxima geração (PA-Series, VM-Series) e interfaces da *web Panorama, Prisma Access.* No caso de *GlobalProtect Gateways, GlobalProtect Portal, Clientless VPN, Captive Portal e Prisma Access*, um invasor não autenticado com acesso de rede aos servidores afetados pode obter acesso a recursos protegidos se permitido pela autenticação e segurança configuradas políticas. Não há impacto na integridade e disponibilidade do *gateway*, portal ou servidor VPN. Um invasor não pode inspecionar ou adulterar sessões de usuários regulares. No pior dos casos, esta é uma vulnerabilidade de gravidade crítica com uma pontuação base CVSS de 10,0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H /UM). No caso das interfaces da *web* PAN-OS e *Panorama*, esse problema permite que um invasor não autenticado com acesso de rede às interfaces da *web* PAN-OS ou *Panorama* faça *login* como administrador e execute ações administrativas. Na pior das hipóteses, esta é uma vulnerabilidade de gravidade crítica com uma pontuação básica CVSS de 10,0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I :H/A:H). Se as interfaces da *Web* forem acessíveis apenas a uma rede de gerenciamento restrita, o problema será reduzido para uma pontuação básica CVSS de 9,6 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/ C:H/I:H/A:H). A *Palo Alto Networks* não está ciente de nenhuma tentativa maliciosa de explorar esta vulnerabilidade.
CVE-2019-1579	A execução remota de código no PAN-OS 7.1.18 e anterior, PAN-OS 8.0.11-h1 e anterior e PAN-OS 8.1.2 e anterior com *GlobalProtect Portal* ou *GlobalProtect Gateway Interface* ativado pode permitir que um invasor remoto não autenticado execute código arbitrariamente.

5.8 QNAP:

CVE-2021-28799	Uma vulnerabilidade de autorização imprópria foi relatada para afetar o QNAP NAS executando HBS 3 (*Hybrid Backup Sync*.) Se explorada, a vulnerabilidade permite que invasores remotos façam *login* em um dispositivo. Este problema afeta: *QNAP Systems Inc.* HBS 3 versões anteriores a v16.0.0415 no QTS 4.5.2; versões anteriores a v3.0.210412 no QTS 4.3.6; versões anteriores a v3.0.210411 no QTS 4.3.4; versões anteriores a v3.0.210411 no QTS 4.3.3; versões anteriores à v16.0.0419 no QuTS hero h4.5.1; versões anteriores a v16.0.0419 no *QuTScloud* c4.5.1~c4.5.4. Este problema não afeta: *QNAP Systems Inc.* HBS 2 . *QNAP Systems Inc.* HBS 1.3 .
CVE-2020-36198	Foi relatado que uma vulnerabilidade de injeção de comando afeta certas versões do *Malware Remover*. Se explorada, esta vulnerabilidade permite que atacantes remotos executem comandos arbitrários. Este problema afeta: *QNAP Systems Inc*. Versões do *Malware Remover* anteriores a 4.6.1.0. Este problema não afeta: *QNAP Systems Inc. Malware Remover* 3.x.

5.9 SOPHOS:

CVE-2020-12271	Um problema de injeção de SQL foi encontrado no SFOS 17.0, 17.1, 17.5 e 18.0 antes de 2020-04-25 em dispositivos *Sophos XG Firewall*, conforme explorado em estado selvagem em abril de 2020. Isso afetou os dispositivos configurados com o serviço de administração (HTTPS) ou o Portal do Usuário exposto na zona WAN. Um ataque bem-sucedido pode ter causado a execução remota de código que exfiltrou nomes de usuário e senhas com *hash* para os administradores do dispositivo local, administradores do portal e contas de usuário usadas para acesso remoto (mas não *Active Directory* externo ou senhas LDAP).

5.10 SHAREPOINT:

CVE-2019-0604	Existe uma vulnerabilidade de execução remota de código no *Microsoft SharePoint* quando o *software* falha ao verificar a marcação de origem de um pacote de aplicativo, também conhecida como 'Vulnerabilidade de execução remota de código do *Microsoft SharePoint*'. Este ID CVE é exclusivo de CVE-2019-0594.

5.11 MICROSOFT WINDOWS:

CVE-2019-0708	Existe uma vulnerabilidade de execução remota de código nos Serviços de Área de Trabalho Remota, anteriormente conhecidos como Serviços de Terminal, quando um invasor não autenticado se conecta ao sistema de destino usando RDP e envia solicitações especialmente criadas, também conhecidas como 'Vulnerabilidade de Execução Remota de Código nos Serviços de Área de Trabalho Remota'.
CVE-2020-1472	Existe uma vulnerabilidade de elevação de privilégio quando um invasor estabelece uma conexão de canal seguro de *logon* de rede vulnerável a um controlador de domínio, usando o protocolo remoto de *logon* de rede (MS-NRPC), também conhecido como 'Vulnerabilidade de elevação de privilégio de *logon* de rede'.
CVE-2021-31166	Vulnerabilidade de execução remota de código de pilha de protocolo HTTP.
CVE-2021-36942	Vulnerabilidade de falsificação de LSA do Windows.

5.12 MICROSOFT OFFICE:

CVE-2017-0199	Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1 permitem que invasores remotos executem código arbitrário por meio de um documento criado, também conhecido como "Microsoft Vulnerabilidade de execução remota de código do Office/WordPad com API do Windows."
CVE-2017-11882	O Microsoft Office 2007 *Service Pack* 3, o Microsoft Office 2010 *Service Pack* 2, o Microsoft Office 2013 *Service Pack* 1 e o Microsoft Office 2016 permitem que um invasor execute um código arbitrário no contexto do usuário atual, falhando em lidar adequadamente com objetos na memória, também conhecido como " Vulnerabilidade de corrupção de memória do Microsoft Office". Este ID CVE é exclusivo de CVE-2017-11884.
CVE-2021-40444	Vulnerabilidade de execução remota de código Microsoft MSHTML

5.13 vCENTER:

CVE-2021-21985	O *vSphere Client* (HTML5) contém uma vulnerabilidade de execução remota de código devido à falta de validação de entrada no *plug-in Virtual SAN Health Check*, que é ativado por padrão no vCenter *Server*. Um ator mal-intencionado com acesso de rede à porta 443 pode explorar esse problema para executar comandos com privilégios irrestritos no sistema operacional subjacente que hospeda o vCenter *Server*.

5.14 ACCELLION:

CVE-2021-27101	O Accellion FTA 9_12_370 e anteriores são afetados pela injeção de SQL por meio de um cabeçalho *Host* criado em uma solicitação para *document_root.html*. A versão corrigida é FTA_9_12_380 e posterior.
CVE-2021-27104	O Accellion FTA 9_12_370 e anteriores são afetados pela execução de comandos do sistema operacional por meio de uma solicitação POST criada para vários terminais administrativos. A versão corrigida é FTA_9_12_380 e posterior.
CVE-2021-27102	O Accellion FTA 9_12_411 e anteriores são afetados pela execução de comandos do sistema operacional por meio de uma chamada de serviço da *Web* local. A versão corrigida é FTA_9_12_416 e posterior.
CVE-2021-27103	Accellion FTA 9_12_411 e anteriores são afetados por SSRF por meio de uma solicitação POST criada para wmProgressstat.html. A versão corrigida é FTA_9_12_416 e posterior.

5.15 FILEZEN:

CVE-2021-20655	FileZen (V3.0.0 a V4.2.7 e V5.0.0 a V5.0.2) permite que um invasor remoto com direitos de administrador execute comandos arbitrários do sistema operacional por meio de vetores não especificados.

5.16 ATLASSIAN:

CVE-2021-26084	Nas versões afetadas do *Confluence Server* e do *Data Center*, existe uma vulnerabilidade de injeção OGNL que permitiria que um invasor não autenticado executasse código arbitrário em uma instância do *Confluence Server* ou do *Data Center*. As versões afetadas são antes da versão 6.13.23, da versão 6.14.0 antes da 7.4.11, da versão 7.5.0 antes da 7.11.6 e da versão 7.12.0 antes da 7.12.5.

5.17 ZOHO CORP.:

CVE-2021-40539	O Zoho *ManageEngine ADSelfService Plus* versão 6113 e anteriores é vulnerável ao desvio de autenticação da API *REST* com execução de código remoto resultante.

5.18 MICROSOFT AZURE:

CVE-2021-38647	Vulnerabilidade de execução remota de código da infraestrutura de gerenciamento aberto.

6 RECOMENDAÇÕES ISH

As vulnerabilidades, mesmo as mais antigas, acabam por nunca desaparecer, o que pode tirar muitas noites de sono de profissionais de segurança. Porém, o alerta que deixamos é para que se conheça as vulnerabilidades existentes em seus ambientes antes mesmos que criminosos cibernéticos as descubram, já que ao ponto de vista do atacante, utilizar vulnerabilidades antigas é menos trabalhoso e mais viável do que efetuar explorações e novas falhas *0-day.*

Diante disso, listamos abaixo algumas das melhores práticas para os profissionais de segurança voltadas à defesa de explorações de vulnerabilidades e demais vetores de ataques existentes.

1. Utilização de método de segundo fator para autenticação, sendo recomendado implantar medidas de MFA para contas de administrador ou demais contas utilizadas na organização.
2. Utilização de ferramentas de segurança, como *Anti-malware*, *Endpoints*, DLP e outras ferramentas disponíveis ao mercado, visando proteger o perímetro dos dispositivos da empresa.
3. Manter sistemas e aplicações atualizadas, já que é recomendado que o inventário de *software* seja constantemente realizado, acompanhando o suporte para os produtos, verificando se este não foi encerrado.

Estas são algumas das principais recomendações, podendo e existindo outras cabíveis de acordo com o ambiente de sua organização.

7 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **GTI *by* ISH Tecnologia**
- https://resources.infosecinstitute.com/topic/most-dangerous-vulnerabilities-exploited/
- https://devco.re/blog/2021/08/06/a-new-attack-surface-on-MS-exchange-part-1-Proxy*Logon*/
- https://www.microsoft.com/en-us/security/blog/2020/11/30/zero*logon*-is-now-detected-by-microsoft-defender-for-identity/
- https://www.vmware.com/security/advisories/VMSA-2021-0002.html
- https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429
- https://www.sentinelone.com/blog/enterprise-security-essentials-top-15-most-routinely-exploited-vulnerabilities-2022/
- https://cve.mitre.org/index.html

heimdall
security research
A DIVISION OF ISH