# heimdall

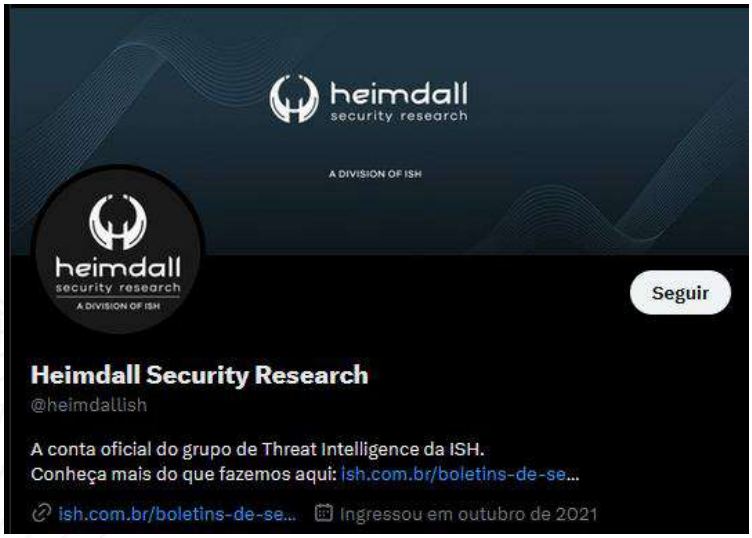
## security research

A DIVISION OF ISH

# Vulnerabilidades identificadas como as mais exploradas em 2022

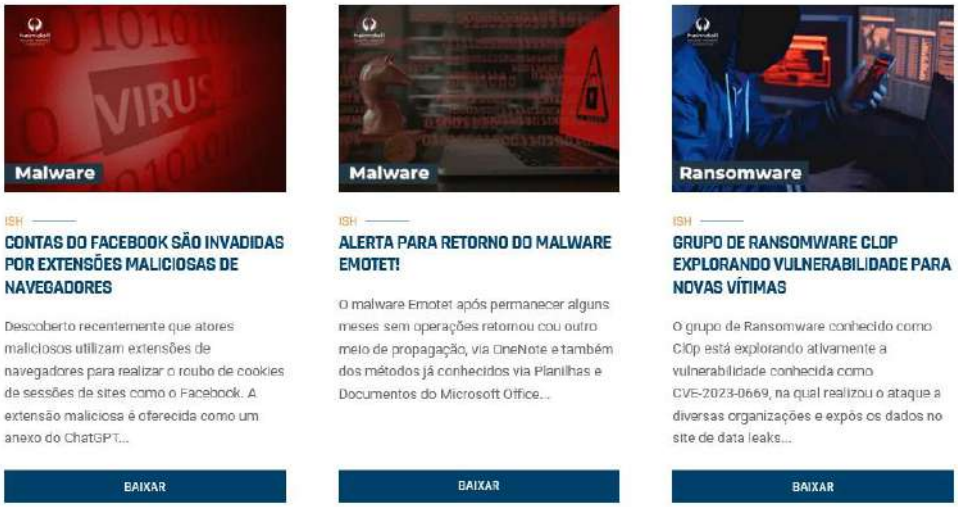
Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

**Heimdall Security Research**




Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

**Boletins de Segurança – Heimdall**



## Sumário

# Lista de Figuras

# 1 INTRODUÇÃO

As organizações modernas dependem cada vez mais da tecnologia da informação (TI) para impulsionar suas operações, fornecer serviços e atender às demandas dos clientes. No entanto, essa crescente dependência também traz consigo uma série de riscos de segurança cibernética, especialmente quando vulnerabilidades não corrigidas em suas infraestruturas de TI são exploradas por atacantes maliciosos. Esses riscos podem ter consequências devastadoras para as organizações, incluindo perdas financeiras, danos à reputação e violações de privacidade.

Tendo em mente isso, recentemente a CISA, NSA e o FBI publicaram uma lista com as **12 vulnerabilidades mais exploradas por atores de ameaças** ao longo do ano de 2022 com o intuito de conscientizar as organizações e governos para as correções dessas vulnerabilidades em suas infraestruturas, dificultando assim os ataques cibernéticos.

## 2 LISTA DA VULNERABILIDADES EXPLORADAS

Abaixo segue imagem e descrição das 12 principais vulnerabilidades que foram observadas e exploradas por atores mal-intencionados em 2022:

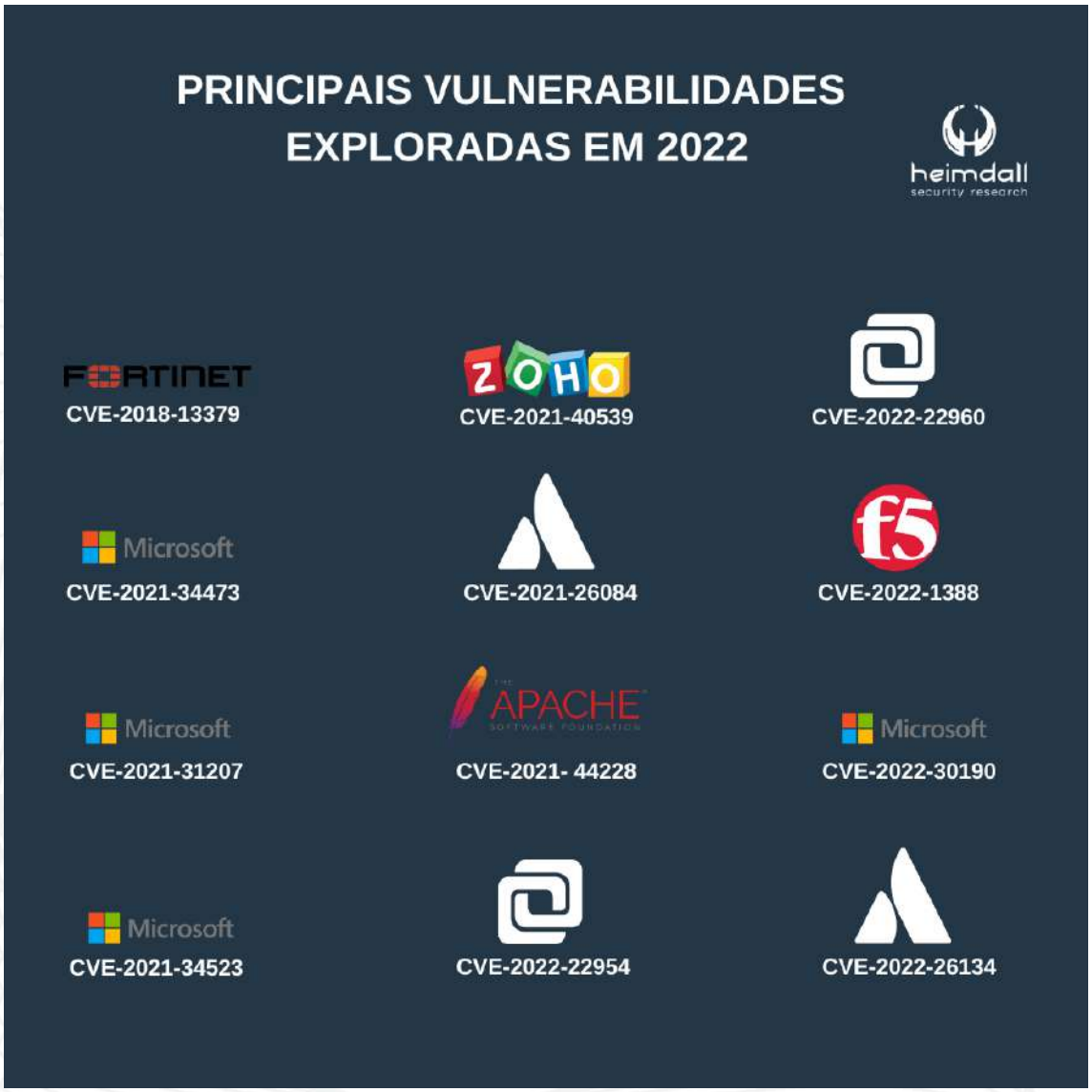



*Figura 1 – Lista das principais vulnerabilidades exploradas em 2022.*

**CVE-2018-13379**, essa vulnerabilidade afeta as VPNs SSL da Fortinet, também foi explorada rotineiramente em 2020 e 2021. A exploração contínua indica que muitas organizações falharam em corrigir o software em tempo hábil e permanecem vulneráveis a agentes cibernéticos mal-intencionados.

**CVE-2021-34473**, **CVE-2021-31207**, **CVE-2021-34523**, essas vulnerabilidades conhecidas como ProxyShell, afetam os servidores de e-mail do Microsoft Exchange. Em combinação, a exploração bem-sucedida permite que um ator remoto execute código arbitrário. Essas vulnerabilidades residem no Microsoft Client Access Service (CAS), que geralmente é executado na porta 443 no Microsoft Internet Information Services (IIS) (por exemplo, servidor da Web da Microsoft). O CAS é comumente exposto à Internet para permitir que os usuários acessem seus e-mails por meio de dispositivos móveis e navegadores da web.

**CVE-2021-40539**, vulnerabilidade permite a execução remota de código não autenticado (RCE) no Zoho ManageEngine ADSelfService Plus e foi vinculada ao uso de uma dependência desatualizada de terceiros. A exploração inicial dessa vulnerabilidade começou no final de 2021 e continuou ao longo de 2022.

**CVE-2021-26084**, essa vulnerabilidade afeta o Atlassian Confluence Server and Data Center (uma ferramenta de colaboração baseada na Web usada por governos e empresas privadas), pode permitir que um agente cibernético não autenticado execute código arbitrário em sistemas vulneráveis. Essa vulnerabilidade rapidamente se tornou uma das vulnerabilidades mais exploradas rotineiramente depois que uma PoC foi lançada uma semana após sua divulgação. A tentativa de exploração em massa dessa vulnerabilidade foi observada em setembro de 2021.

**CVE-2021-44228**, conhecida como Log4Shell, afeta a biblioteca Log4j do Apache, uma estrutura de log de código aberto incorporada a milhares de produtos em todo o mundo. Um ator pode explorar essa vulnerabilidade enviando uma solicitação especialmente criada a um sistema vulnerável, causando a execução de código arbitrário. A solicitação permite que um ator cibernético assuma o controle total de um sistema. O ator pode roubar informações, lançar ransomware ou realizar outras atividades maliciosas. Atores cibernéticos mal-intencionados começaram a explorar a vulnerabilidade depois que ela foi divulgada publicamente em dezembro de 2021 e continuaram a demonstrar grande interesse no CVE-2021-44228 até o primeiro semestre de 2022.

**CVE-2022-22954**, **CVE-2022-22960**, essas vulnerabilidades permitem RCE, escalonamento de privilégios e bypass de autenticação no VMware Workspace ONE Access, Identity Manager e outros produtos VMware. Um agente cibernético mal-intencionado com acesso à rede pode acionar uma injeção de modelo do lado do servidor que pode resultar na execução

remota de código. A exploração de CVE-2022-22954 e CVE-2022-22960 começou no início de 2022 e as tentativas continuaram durante o restante do ano.

**CVE-2022-1388**, uma vulnerabilidade permite que atores cibernéticos mal-intencionados não autenticados ignorem a autenticação iControl REST na entrega de aplicativos F5 BIG-IP e no software de segurança.

**CVE-2022-30190**, vulnerabilidade que afeta a Ferramenta de diagnóstico de suporte da Microsoft (MSDT) no Windows. Um ator cibernético remoto e não autenticado pode explorar essa vulnerabilidade para assumir o controle de um sistema afetado.

**CVE-2022-26134**, essa é uma vulnerabilidade crítica do RCE afeta o Atlassian Confluence e o Data Center. A vulnerabilidade, que provavelmente foi inicialmente explorada como um dia zero antes da divulgação pública em junho de 2022, está relacionada a uma vulnerabilidade mais antiga do Confluence (CVE-2021-26084), que os cibercriminosos também exploraram em 2022.

*OBS. Informamos que estas vulnerabilidades se encontram no catálogo de vulnerabilidades exploradas conhecidas da CISA devido a suas explorações por cibercriminosos em ataques cibernéticos.*

# 3 Conclusão

As organizações que possuem vulnerabilidades exploradas em suas infraestruturas de TI estão sujeitas a diversos riscos de segurança significativos, que podem ter impactos negativos tanto em termos financeiros quanto na reputação da empresa.

A **segurança cibernética deve ser tratada como uma prioridade contínua para as organizações**, pois os riscos de vulnerabilidades exploradas podem mudar rapidamente com o cenário de ameaças em constante evolução.

# 4 RECOMENDAÇÕES

Listadas pela ISH, as medidas abaixo poderão ser adotadas visando a mitigação das referidas *vulnerabilidades*, como por exemplo:

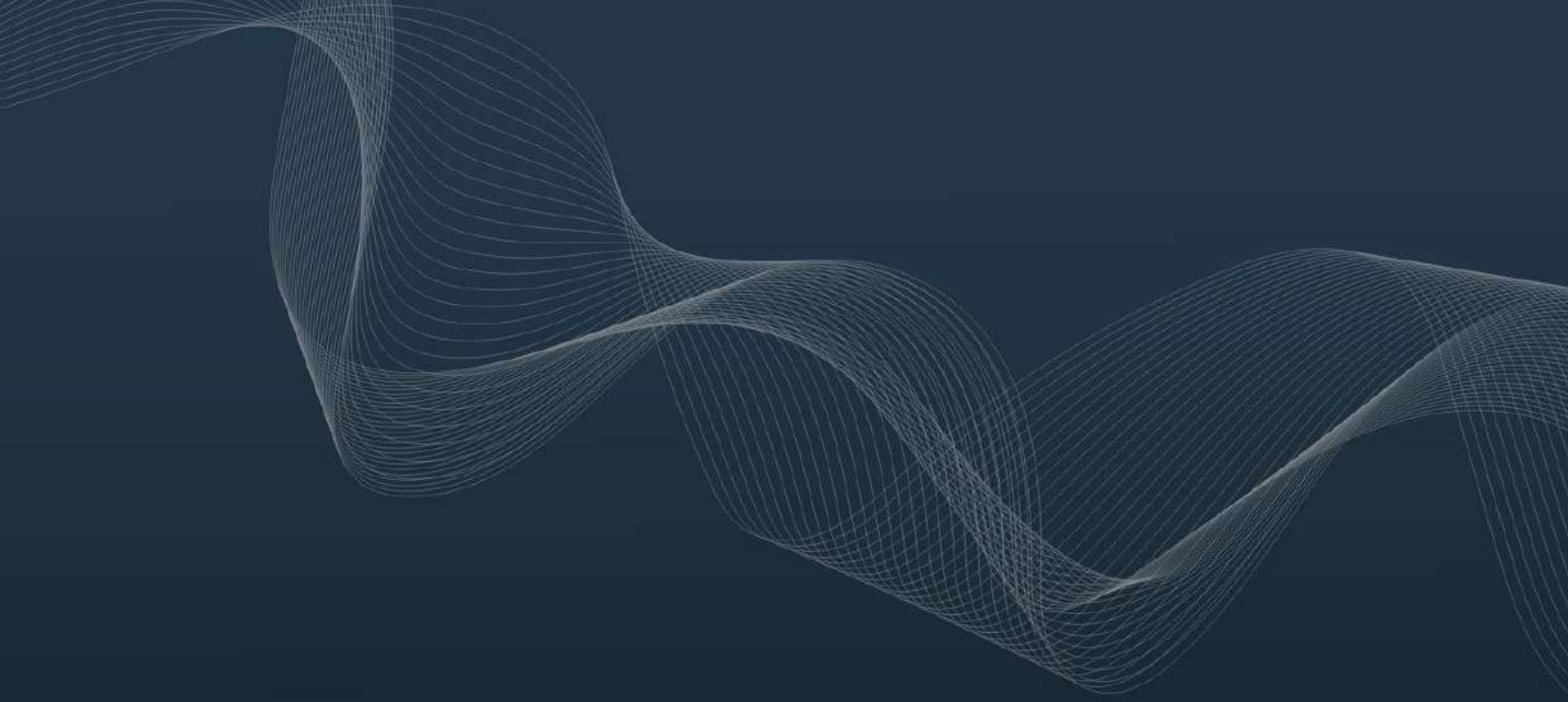
- **Mantenha sistemas e software atualizados**, certifique-se de que todos os sistemas, aplicativos e dispositivos estejam atualizados com as últimas correções de segurança e patches disponibilizados pelos fornecedores. Muitas vulnerabilidades são corrigidas por meio de atualizações, portanto, manter-se atualizado é uma medida fundamental de segurança.
- **Implemente uma defesa em camadas**, use uma abordagem de segurança em camadas para proteger sua infraestrutura de TI. Isso inclui a utilização de firewalls, antivírus, detecção de intrusões, prevenção de intrusões, autenticação multifator e outras soluções de segurança para proteger contra várias ameaças.
- **Realize avaliações regulares de segurança**, realize testes de penetração e avaliações de vulnerabilidades regularmente para identificar e corrigir possíveis vulnerabilidades em sua infraestrutura antes que sejam exploradas por atacantes.
- **Monitore ativamente os logs de segurança**, implemente um sistema de monitoramento de segurança que rastreie e analise regularmente os logs de eventos para detectar atividades suspeitas ou não autorizadas em sua rede. Isso pode ajudar a identificar ameaças em estágio inicial.
- **Treine e conscientize os funcionários**, eduque os funcionários sobre práticas seguras de computação e os riscos associados a ataques cibernéticos, incluindo phishing e engenharia social. Funcionários bem treinados são a primeira linha de defesa contra muitos ataques.
- **Faça backup regularmente**, realize backups regulares de seus dados importantes e verifique se eles são armazenados de forma segura. Em caso de ataque de ransomware ou perda de dados, ter backups disponíveis pode ser uma forma de recuperação.
- **Implemente políticas de acesso e controle de privilégios**, restrinja o acesso a dados confidenciais e recursos críticos apenas para as pessoas autorizadas e com necessidade de acesso. Isso reduzirá o risco de acesso não autorizado.

- **Utilize criptografia**, use criptografia para proteger dados em trânsito e em repouso. Isso torna mais difícil para os invasores acessarem informações confidenciais.
- **Estabeleça planos de resposta a incidentes**, tenha um bom plano de resposta a incidentes em vigor, definindo procedimentos claros para identificar, conter, erradicar e recuperar-se de ataques cibernéticos.
- **Avalie fornecedores e terceiros**, se você compartilha informações ou dados com terceiros, verifique a segurança de suas práticas para garantir que eles também estejam protegendo suas informações adequadamente.

*Mais informações sobre recomendações e mitigações sobre as vulnerabilidades exploradas podem ser encontradas na página oficial da CISA no tópico mitigações.*

# 5 REFERÊNCIAS


- **Heimdall *by* ISH Tecnologia**
- **CISA**



heimdall
security research

A DIVISION OF ISH