Tempest

ACADEMY

Conference

2023

Vulnerabilidades Vintage

O que são e como enfrentar

Classificação da Informação: PÚBLICA
Autor da apresentação: Diego Patrik

01 Definindo Vulnerabilidades Vintage

02 Analisando alguns exemplos

03 Principais vulnerabilidades do ano passado

04 Relação com Ransomware

05 Como enfrentar o problema

Tempest

:ACADEMY:

Conference

Diego Patrik

Analista de Cibersegurança, com foco em Gestão de Vulnerabilidades.
Faz parte do time de Gestão de Vulnerabilidades e Compliance (GVC) da Tempest.

Tem interesse em Threat Intelligence e Cloud.
Para os dias livres escolhe viagens, jogos e vinhos.

Tempest

[ACADEMY]

Conference

Definindo Vulnerabilidades Vintage

Tempest

:ACADEMY:

Conference

Definição: Vulnerabilidade

Usaremos a definição no contexto cibernético, sendo uma falha de segurança que pode ser explorada por ameaças, servindo como brechas para diversos tipos de ataques.

Tempest
:ACADEMY:
Conference

Definição: Vintage

A tradução literal é vindima (“colheita”), a origem vem de *vint*, que significa safra de uvas, e *age*, de idade.

Antigamente, o termo era usado para vinhos produzidos com as melhores colheitas e que eram envelhecidos.

A ideia se estendeu para moda, design e em seguida para qualquer produto ou objeto...

Usaremos a definição mais popular atualmente, de algo clássico, antigo e de boa qualidade.

Vulnerabilidades Vintage

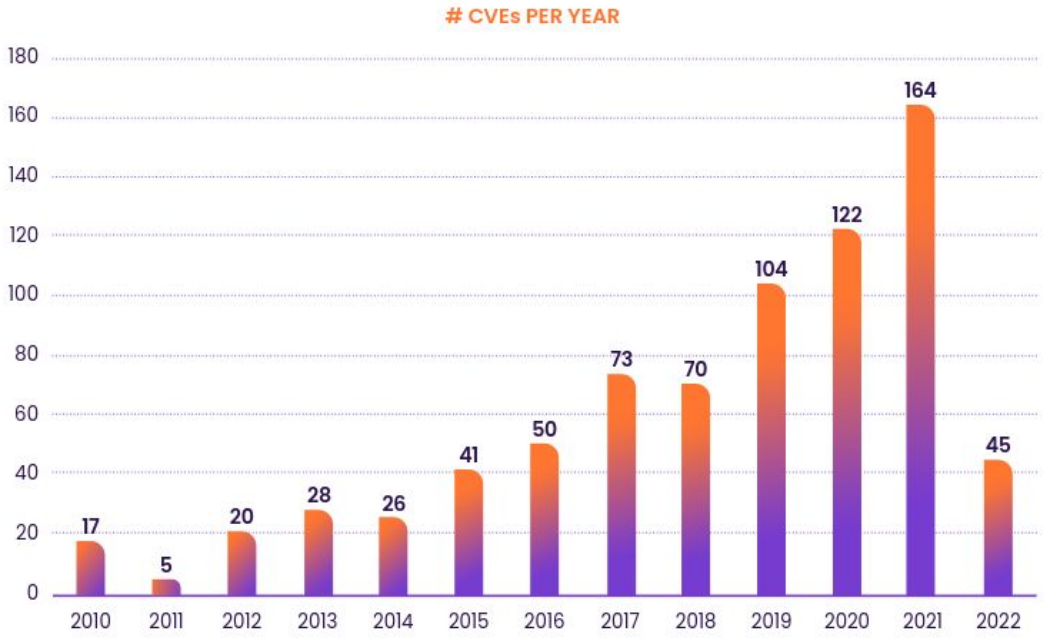
Tempest
[ACADEMY]
Conference

Resumindo...

- ➔ Vulnerabilidades antigas
- ➔ com patch disponível
- ➔ alta severidade técnica
- ➔ ativamente exploradas
- ➔ seguem sem aplicação da correção

CISA: Known Exploited Vulnerabilities (KEV)

Tempest
ACADEMY
Conference



Fonte: Rezilion

Vulnerabilidade: tempo de vida

Tempest
[ACADEMY]
Conference

Fonte: Rezilion

Tempest
[ACADEMY]
Conference

Corrigir deveria ser a parte fácil

Os adversários não se preocupam em estarem fora da moda.

Se consideramos irrelevantes vulnerabilidades identificadas e corrigidas pelos fabricantes anos atrás, e que são conhecidas por serem exploradas há anos, então estamos jogando do lado deles!

Tempest
[ACADEMY]
Conference

“low-hanging fruit”

Fonte: clydestyle.org

Tempest

ACADEMY

Conference

Analisando alguns exemplos

Vulnerabilidades vintage mencionadas em 2023

Tempest
[ACADEMY]
Conference

Tempest
[ACADEMY]
Conference

Adicionadas no catálogo da CISA no dia **12/05/2023**
e mencionadas no Podcast Cyber Morning Call

Vulnerabilidade	**CVSS Base**	**Tipo**	**Correção disponível**
Oracle Java SE and JRockit Unspecified Vulnerability (CVE-2016-3427)	9.0	Não especificado	desde 2016
CVE-2016-8735 Apache Tomcat Remote Code Execution Vulnerability	9.8	RCE	desde 2016

Tempest
[ACADEMY]
Conference

medium.com
https://medium.com › achieving-r... · Traduzir esta página

Achieving RCE on Tomcat via CVE-2016-8735 - Medium

8 de mar. de 2019 — In this post I will outline the process of developing an exploit for a vulnerability (**CVE-2016–8735**) in the popular servlet container ...

Exemplificando como casos antigos podem voltar a serem relevantes...

Tempest ACADEMY Conference

Vulnerabilities/Threats | 6 MIN READ | NEWS

Microsoft Patches 'Follina' Zero-Day Flaw in Monthly Security Update

Here are which Microsoft patches to prioritize among the June Patch Tuesday batch.

Jai Vijayan
Contributing Writer, Dark Reading

June 14, 2022

Threat Intelligence | 4 MIN READ | NEWS

Microsoft Follina Bug Is Back in Meme-Themed Cyberattacks Against Travel Orgs

A two-bit comedian is using a patched Microsoft vulnerability to attack the hospitality industry, and really laying it on thick along the way.

Nate Nelson
Contributing Writer, Dark Reading

May 15, 2023

Fonte: Dark Reading

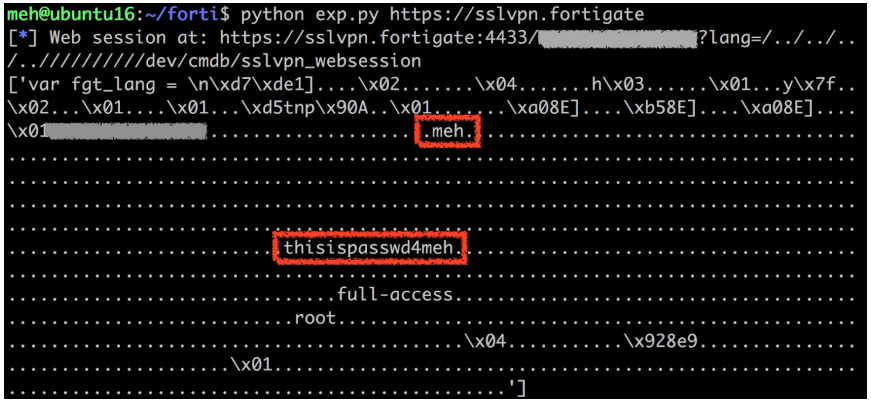
CVE-2018-13379

Tempest
[ACADEMY]
Conference

CVE-2018-13379 — Fortinet FortiOS and FortiProxy
CVSS3 — 9.8
Conhecida por ser ativamente explorada — Sim
Idade da Vuln: 5 Anos

Vulnerabilidade do tipo "*Path traversal*" no portal web do FortiProxy SSL VPN, permite ao atacante obter arquivos de configuração e no cenário em questão, as credenciais de usuários locais de appliances Fortigate em texto plano.

Data do patch: 24 de Maio de 2019.



Fonte: devcore

Tempest
[ACADEMY]
Conference

Centenas de empresas brasileiras permanecem vulneráveis ao CVE-2018–13379

OpenCTIBR · Follow
Published in OpenCTI.BR · 3 min read · Jun 9

Recentemente foi divulgado em um fórum hacker, uma lista contendo aproximadamente 51 mil endereços IPs vulneráveis à CVE-2018–13379. Esta vulnerabilidade, do tipo "Path traversal" permite ao atacante obter arquivos de configuração e no cenário em questão, as credenciais de usuários locais de appliances Fortigate.

Este artetafo foi citado em blog especializado em Nov/2020, conforme o link a seguir. (https://secrutiny.com/2020/11/hacker-posts-exploits-exposes-passwords-for-vulnerable-fortinet-vpns/)

Fonte: OpenCTI.BR

Tempest ACADEMY Conference

JOINT
CYBERSECURITY ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA21-092A

April 2, 2021

APT Actors Exploit Vulnerabilities to Gain Initial Access for Future Attacks

SUMMARY

In March 2021 the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) observed Advanced Persistent Threat (APT) actors scanning devices on ports 4443, 8443, and 10443 for CVE-2018-13379, and enumerated devices for CVE-2020-12812 and CVE-2019-5591. It is likely that the APT actors are scanning for these vulnerabilities to gain access to multiple government, commercial, and technology services networks. APT actors have historically exploited critical vulnerabilities to conduct distributed denial-of-service (DDoS) attacks, ransomware attacks, structured query language (SQL) injection attacks, spearphishing campaigns, website defacements, and disinformation campaigns.

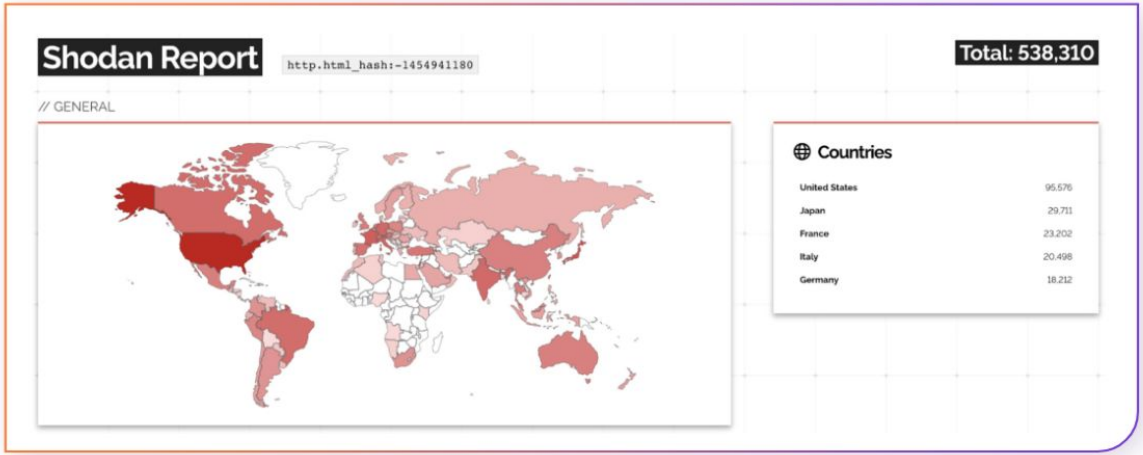
TECHNICAL DETAILS

The FBI and CISA have information indicating APT actors are using multiple CVEs to exploit Fortinet FortiOS vulnerabilities. The FBI and CISA believe the APT actors are likely exploiting these Fortinet FortiOS vulnerabilities—CVE 2018-13379, CVE-2020-12812, and CVE-2019-5591—to gain access to multiple government, commercial, and technology services networks.

The APT actors may be using any or all of these CVEs to gain access to networks across multiple critical infrastructure sectors to gain access to key networks as pre-positioning for follow-on data exfiltration or data encryption attacks. APT actors may use other CVEs or common exploitation techniques—such as spearphishing—to gain access to critical infrastructure networks to pre-position for follow-on attacks.

De 2019 até 2023...

Tempest
[ACADEMY]
Conference



Fonte: Rezilion (ago/22)

Finalizando com um caso que reforça ainda mais a importância do tema:

Tempest [ACADEMY] Conference

CYBERSECURITY ADVISORY

Threat Actors Exploit Progress Telerik Vulnerability in U.S. Government IIS Server

Release Date: March 15, 2023 **Alert Code:** AA23-074A

SUMMARY

From November 2022 through early January 2023, the Cybersecurity and Infrastructure Security Agency (CISA) and authoring organizations identified the presence of indicators of compromise (IOCs) at a federal civilian executive branch (FCEB) agency. Analysts determined that multiple cyber threat actors, including an APT actor, were able to exploit a .NET deserialization vulnerability (CVE-2019-18935) in Progress Telerik user interface (UI) for ASP.NET AJAX, located in the agency's Microsoft Internet Information Services (IIS) web server. Successful exploitation of this vulnerability allows for remote code execution. According to Progress Software, Telerik UI for ASP.NET AJAX builds before R1 2020 (2020.1.114) are vulnerable to this exploit.[1]

Fonte: CISA

Recentemente, dados de uma agência federal, FCEB (Federal Civilian Executive Branch), foram roubados.

Os atacantes obtiveram um RCE **explorando um bug antigo (CVE-2019-18935)** em um servidor web IIS da agência, tendo acesso entre Novembro de 2022 e Janeiro de 2023.

Tempest

[ACADEMY]

Conference

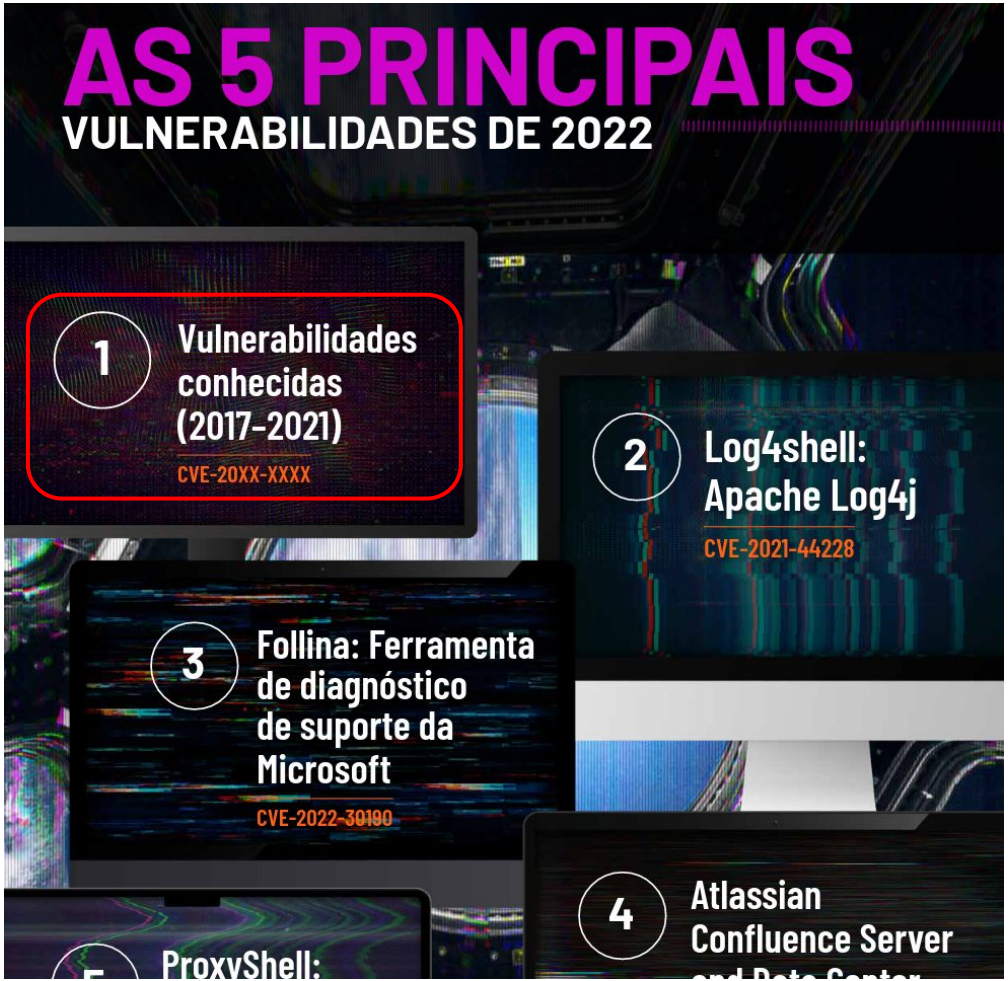
Principais vulnerabilidades de 2022

Relatório da Tenable

Tempest
[ACADEMY]
Conference

O mais alarmante, talvez, seja que, junto com a grande quantidade de novas vulnerabilidades descobertas em 2022, as **vulnerabilidades de anos anteriores continuam assombrando** as organizações. Na verdade, **as falhas desde 2017 foram tão proeminentes este ano que achamos que elas merecem um lugar na lista** das principais vulnerabilidades de 2022.

– Tenable



Tempest
ACADEMY
Conference

Fonte: Relatório do Cenário de Ameaças de 2022 da Tenable

Tempest
ACADEMY
Conference

A Tenable citou em seu relatório as seguintes vulnerabilidades antigas que também se destacaram entre as exploradas em ataques no ano de 2022

CVE	Produto afetado	Descrição	CVSSv3
CVE-2017-11882	Microsoft Office Equation Editor	Corrupção de memória	7,8
CVE-2018-0798	Microsoft Office Equation Editor	Corrupção de memória	8,8
CVE-2018-0802	Microsoft Office Equation Editor	Corrupção de memória	7,8
CVE-2018-13379	Fortinet FortiOS	Travessia de caminho	9,8
CVE-2020-14882	Oracle WebLogic	RCE não autenticado	9,8
CVE-2021-40539	Zoho ManageEngine ADSelfService Plus	Desvio de autenticação para RCE	9,8
CVE-2021-40444	Microsoft MSHTML (Trident)	RCE não autenticado	7,8
CVE-2021-44077	Zoho ManageEngine ServiceDesk Plus	RCE não autenticado	9,8

Visão da Kaspersky

Tempest
[ACADEMY]
Conference

Fonte: Kaspersky

A Kaspersky pontuou sobre o **aumento de ataques usando vulnerabilidades antigas do Microsoft Office** em ataques no Q2 2022

Kaspersky experts found that exploits for the vulnerability, designated CVE-2021-40444, were used to attack almost 5,000 people in Q2 2022, which is eight times more than during Q1 2022. This zero-day vulnerability in Internet Explorer's engine MSHTML was first reported in September 2021. The engine is a system component used by Microsoft Office applications to handle web content. When exploited, it enables the remote execution of malicious code on victims' computers.

Vulnerability	Attacked users in Q2 2022	Dynamics of attacked users, % Q2 2022 vs Q1 2022
CVE-2021-40444	4,886	696%
CVE-2017-0199	60,132	59%
CVE-2017-11882	140,623	5%
CVE-2018-0802	345,827	3%

The comparative number of users affected by Microsoft Office vulnerabilities in Q2 2022, and associated dynamics

Tempest

[ACADEMY]

Conference

Relação com Ransomware

2023 Spotlight Report: Ransomware Through the Lens of Threat and Vulnerability Management

Tempest
[ACADEMY]
Conference

O estudo, que gerou este relatório, foi realizado em conjunto por Cyber Security Works (CSW), Ivanti, Cyware, e Securin listou **76% das vulnerabilidades atualmente exploradas por grupos de ransomware** como **descobertas antes de 2020**. Em 2022, das 56 associadas a ransomware, 20 foram descobertas entre 2015 e 2019.

CVE-2021-21974: Falha corrigida em 2021, sendo usada em ataques de ransomware em 2023

Tempest [ACADEMY] Conference

EXPLOITS AND VULNERABILITIES | NEWS | RANSOMWARE

[update]Two year old vulnerability used in ransomware attack against VMware ESXi

Posted: February 6, 2023 by Pieter Arntz

On Friday and over the weekend, several Computer Emergency Response Teams (CERTs) sounded the alarm about an ongoing large scale ransomware attack on VMware ESXi virtual machines.

With some discrepancies between Shodan queries from various researchers, most agree that an estimated 500 entities were affected by the attack over the weekend.

Fonte: malwarebytes

ESXiArgs | Ataque de ransomware em grande escala já tem vítimas no Brasil

Pelo menos 21 servidores de virtualização disponíveis no Brasil foram atingidos por onda de ransomware que começou no fim de semana e já fez milhares de vítimas

Felipe Demartini

10 fev 2023 - 16h47 (atualizado às 18h35) Compartilhar Ver comentários

Ouvir texto 0:00

Quase uma semana depois de começar em pelo menos cinco países da América do Norte e Europa, os ataques ESXiArgs finalmente começaram a fazer vítimas no Brasil. Entre quinta (09) e esta sexta-feira (10), pelo menos 21 servidores de virtualização baseados na tecnologia caíram sob os golpes de ransomware que vem atingindo infraestruturas de todo o mundo.

Fonte: Terra

Tempest

[ACADEMY]

Conference

Como Enfrentar o Problema

Tempest
[ACADEMY]
Conference

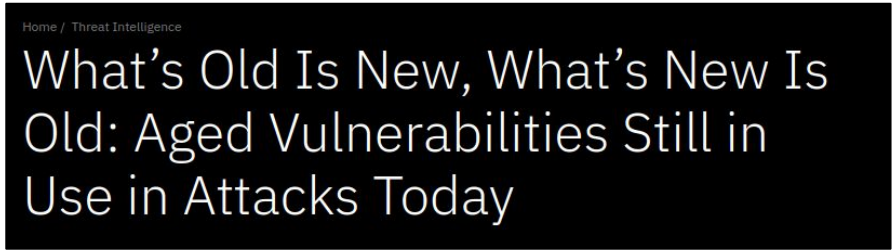
Antes da conclusão, nos perguntamos: **Por que temos esse cenário?**

Resposta rápida: porque patches não são aplicados


VULNERABILITIES

Cisco Warns of Many Old Vulnerabilities Being Exploited in Attacks

Cisco has updated multiple security advisories to warn of the malicious exploitation of severe vulnerabilities impacting its networking devices. Many of the bugs, which carry severity ratings of 'critical' or 'high', have been addressed 4-5 years ago, but organizations that haven't patched their devices continue to be impacted.


Home / Threat Intelligence

What's Old Is New, What's New Is Old: Aged Vulnerabilities Still in Use in Attacks Today


NEWS

Unpatched old vulnerabilities continue to be exploited: Report

The top five exploited vulnerabilities in 2022 include several high-severity flaws in Microsoft Exchange, Zoho ManageEngine products, and virtual private network solutions from Fortinet, Citrix and Pulse Secure.

Separei alguns dos motivos:

Tempest
[ACADEMY]
Conference

- ➔ Atenção elevada somente no início do ciclo de vida da vulnerabilidade
- ➔ Aplicação da correção não é encarada como prioridade
- ➔ Sobrecarga nos times de TI ou falta de pessoal
- ➔ Vuln tão antiga que time “corrigiu mentalmente”, acha que já está corrigido
- ➔ Falta de visibilidade, time sequer tem noção da existência da vulnerabilidade antiga no ambiente
- ➔ Complexidade ou impacto da aplicação do patch
- ➔ Usuários não colaboram com ações necessárias, por exemplo: reiniciar máquina ou aplicação

No fim das contas, não é a idade, mas sim o risco da vulnerabilidade que importa

Com uma **Gestão de Vulnerabilidades baseada em risco**, as **vulnerabilidades antigas de severidade técnica alta e ativamente exploradas** como vimos, **passam a ser também prioridade**, dentro de um número menor das que teremos que corrigir primeiro.

Tempest
[ACADEMY]
Conference

Gestão de Vulnerabilidades

Passo 1

- ➔ Visibilidade contínua do ambiente
- ➔ Priorização com base no risco
- ➔ Definição de SLA para a correção de vulnerabilidades
- ➔ Acompanhamento da idade de cada vuln
- ➔ Alternativas para a aplicação de correção em sistemas legados

+

Threat Intelligence

Passo 2

- ➔ Maior grau de contexto para GV, trazendo a visão de vulnerabilidades antigas que estão sendo exploradas atualmente
- ➔ Monitoramento do surgimento de exploits, aumentando o risco de uma vuln que era considerada de baixa prioridade

+

Pentest

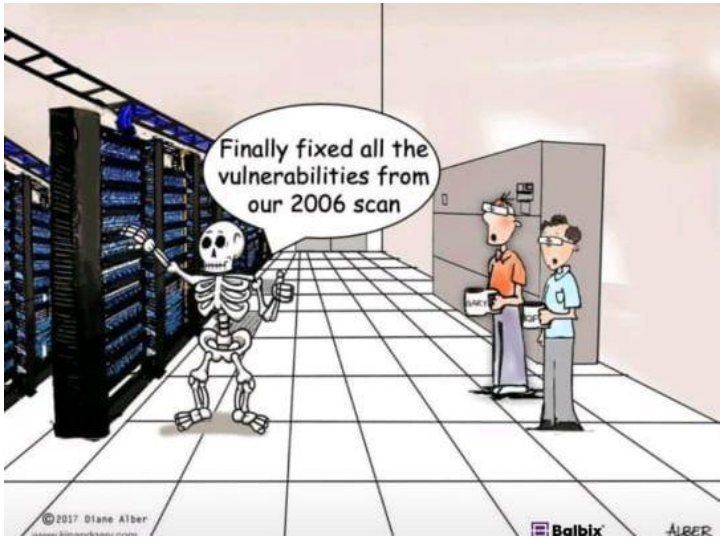
Passo 3

- ➔ Verificar a explorabilidade das vulns encontradas nos scans de GV
- ➔ Confirmar efetividade do patch ou mitigação
- ➔ Testar controles implementados para vulns que não serão corrigidas

Tempest
[ACADEMY]
Conference

Combinar medidas proativas com base em risco e pentest pode ajudar os times de segurança a **apontar e priorizar as falhas de maior risco**, antes que um atacante as possa explorar.

Enquanto tentar corrigir **TUDO** nos levará ao seguinte cenário:



Fonte: Balbix

Referências:

https://www.rezilion.com/blog/report-vintage-vulnerabilities-never-go-out-of-fashion/

https://www.coresecurity.com/blog/vintage-vulnerabilities-new-attacks-can-exploit-old-weaknesses

https://www.techrepublic.com/article/vintage-security-vulnerabilities-still-threaten-businesses/

https://www.businesswire.com/news/home/20230216005161/en/76-of-Vulnerabilities-Currently-Exploited-by-Ransomware-Groups-Were-Discovered-Before-2020-Report-Finds

https://www.brookcourtsolutions.com/how-threat-intelligence-prioritises-risk-in-vulnerability-management/

https://securityintelligence.com/posts/whats-old-is-new-whats-new-is-old-aged-vulnerabilities-still-in-use-in-attacks-today/

https://www.malwarebytes.com/blog/news/2023/02/two-year-old-vulnerability-used-in-ransomware-attack-against-vmware-esxi

https://www.kaspersky.com/about/press-releases/2022_eight-times-more-users-attacked-via-an-old-microsoft-office-vulnerability-in-q2

https://www.darkreading.com/vulnerabilities-threats/the-problem-of-old-vulnerabilities-and-what-to-do-about-it

https://www.bleepingcomputer.com/news/security/us-federal-agency-hacked-using-old-telerik-bug-to-steal-data/

https://open.spotify.com/episode/6lONixE5gAPlb2gOdf6alw?si=8dcdc69e1519436f

Relatório do Cenário de Ameaças de 2022 da Tenable

https://www.terra.com.br/byte/esxiargs-ataque-de-ransomware-em-grande-escala-ja-tem-vitimas-no-brasil,74316636d86f47ce09fda8b3b917c116sltbwstx.html

https://www.coresecurity.com/blog/better-together-how-pen-testing-helps-take-vulnerability-assessments-next-level

https://conceito.de/vintage

https://www.teclasap.com.br/vintage/

Tempest ACADEMY Conference