WTR

WORKSHOP

DE TECNOLOGIA DE REDES DO POP-RS

> 2021

Como o tempo é seu inimigo no tratamento de Incidentes

Rildo Souza

22 SET

PoP-RS

Ponto de Presença da
RNP no Rio Grande do Sul

RNP

ORGANIZAÇÃO SOCIAL DO MCTI

SEGURANÇA DA INFORMAÇÃO NA RNP

CAIS

CSIRT de coordenação da rede acadêmica brasileira.
Gestão da segurança do RNP, backbone e dos clientes da RNP.

Relações Institucionais

Gestão de relacionamento com clientes e parceiros estratégicos da RNP, com o foco em segurança da informação.

Soluções em segurança

Atendimento a demandas por soluções de segurança dos clientes da RNP.
Foco na consultoria de segurança em projetos especiais.

O CAIS

CAIS

Centro de Atendimento a Incidentes de Segurança

Detecção, resolução e prevenção.

Incidentes de Segurança

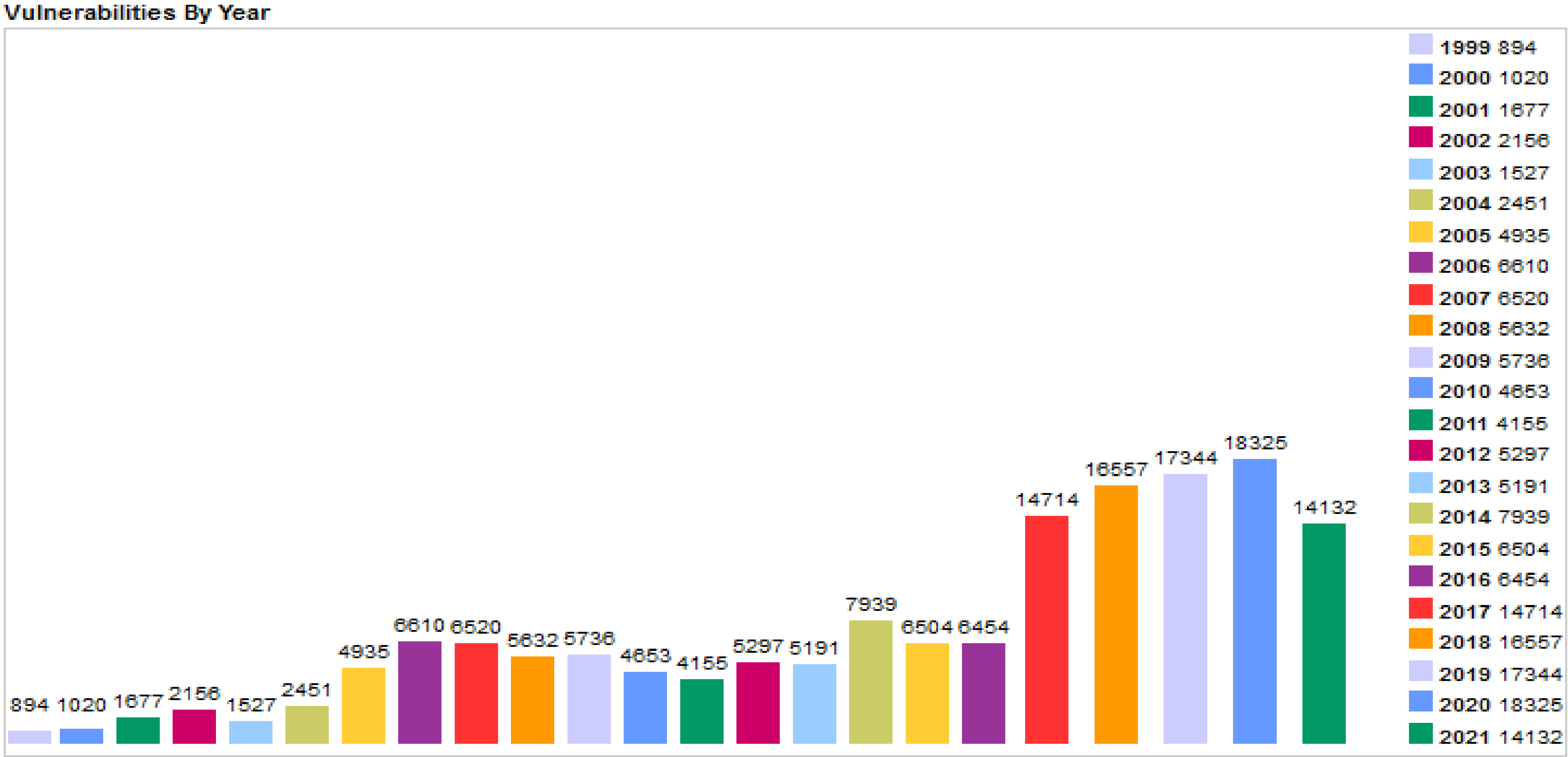
Expertise

Vulnerabilidades de Segurança

Cultura de Segurança

Novos CSIRTs

Vulnerabilidades mundo

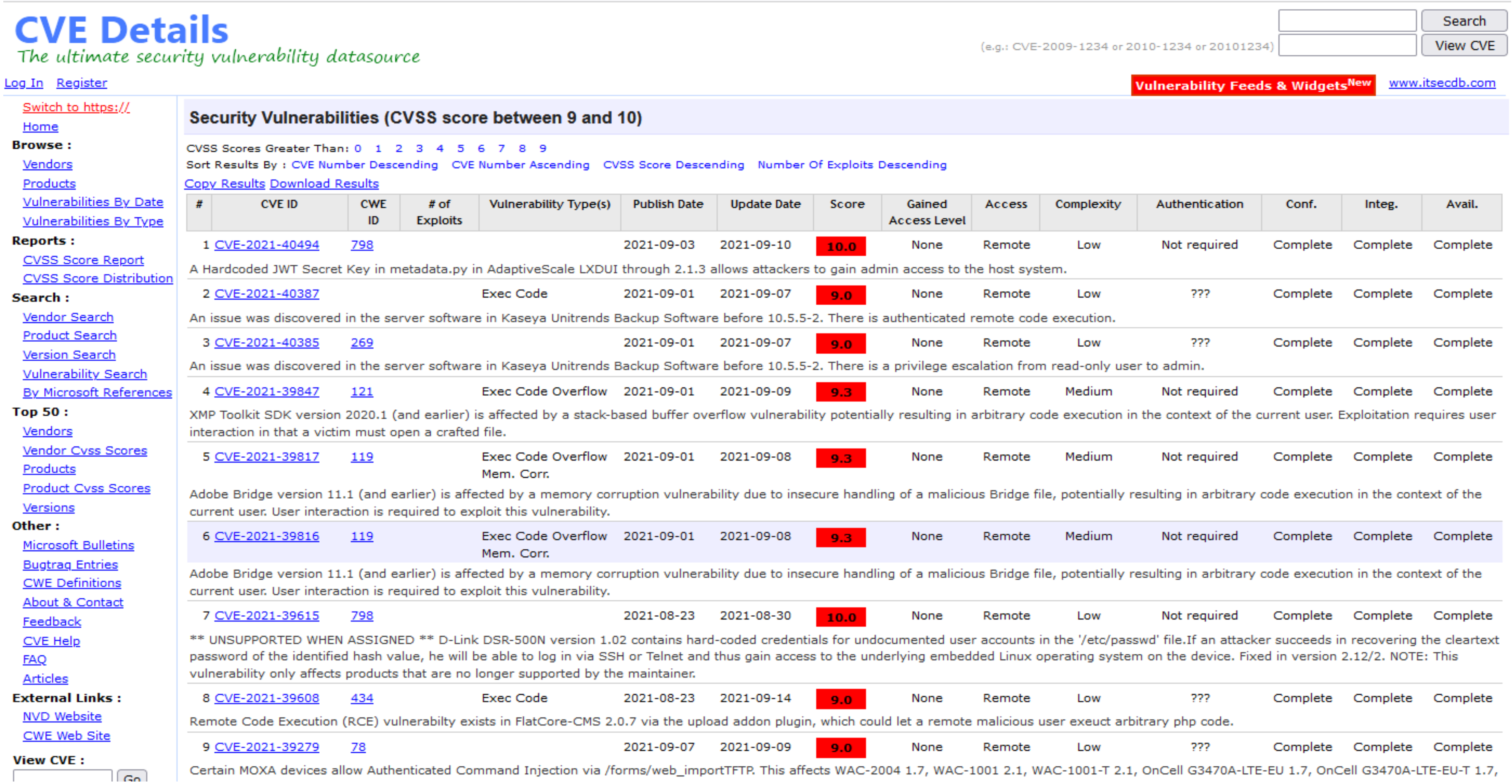


2020 - Média/mês = 1527

2021 - Média/mês = 1570*

Fonte:https://www.cvedetails.com/browse-by-date.php
*Setembro

Vulnerabilidades Críticas



CVE Details
The ultimate security vulnerability datasource

Security Vulnerabilities (CVSS score between 9 and 10)

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

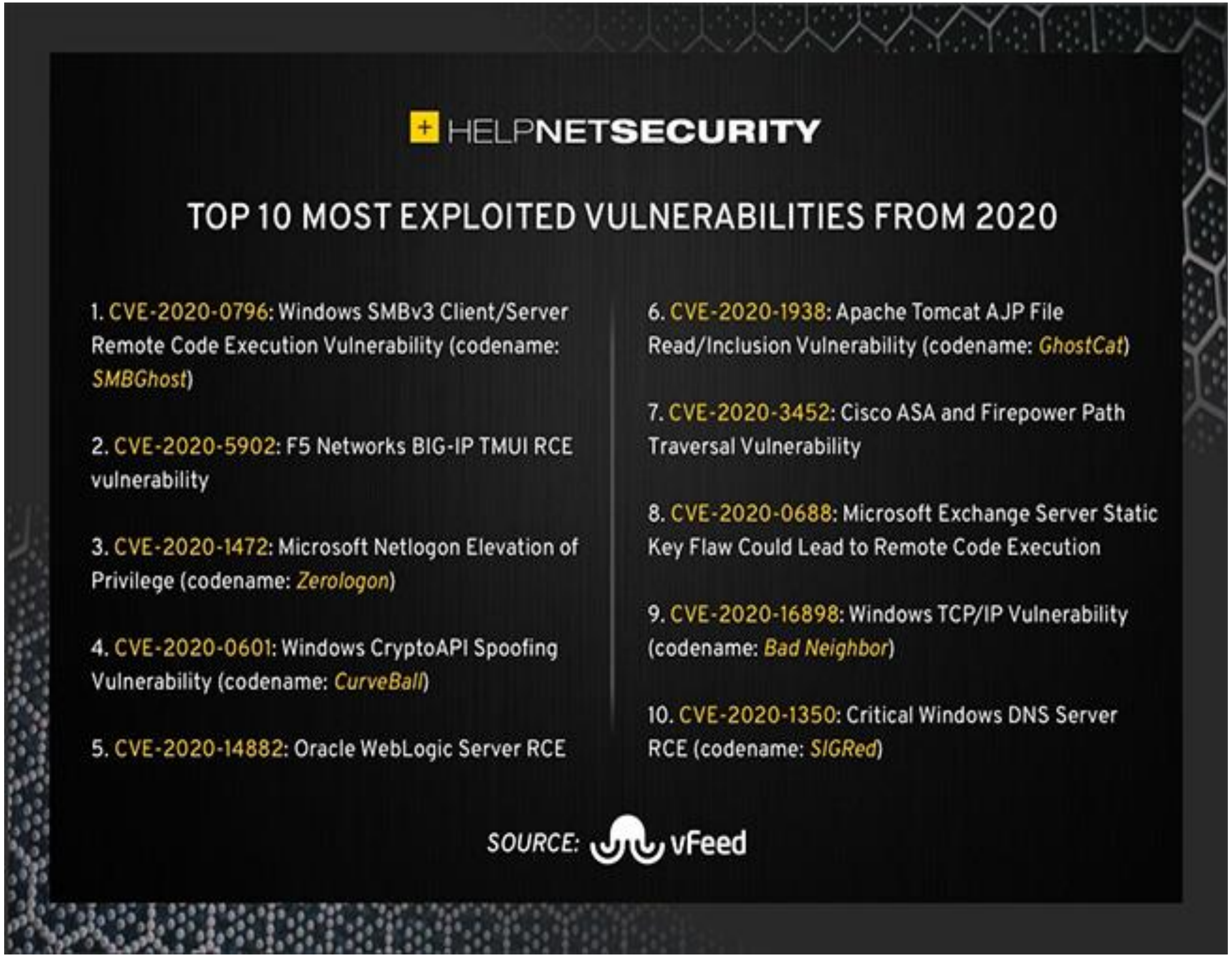
<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexity</th><th>Authentication</th><th>Conf.</th><th>Integ.</th><th>Avail.</th></tr>
<tr><td>1</td><td>CVE-2021-40494</td><td>798</td><td></td><td></td><td>2021-09-03</td><td>2021-09-10</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">A Hardcoded JWT Secret Key in metadata.py in AdaptiveScale LXDUI through 2.1.3 allows attackers to gain admin access to the host system.</td></tr>
<tr><td>2</td><td>CVE-2021-40387</td><td></td><td></td><td>Exec Code</td><td>2021-09-01</td><td>2021-09-07</td><td>9.0</td><td>None</td><td>Remote</td><td>Low</td><td>???</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">An issue was discovered in the server software in Kaseya Unitrends Backup Software before 10.5.5-2. There is authenticated remote code execution.</td></tr>
<tr><td>3</td><td>CVE-2021-40385</td><td>269</td><td></td><td></td><td>2021-09-01</td><td>2021-09-07</td><td>9.0</td><td>None</td><td>Remote</td><td>Low</td><td>???</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">An issue was discovered in the server software in Kaseya Unitrends Backup Software before 10.5.5-2. There is a privilege escalation from read-only user to admin.</td></tr>
<tr><td>4</td><td>CVE-2021-39847</td><td>121</td><td></td><td>Exec Code Overflow</td><td>2021-09-01</td><td>2021-09-09</td><td>9.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">XMP Toolkit SDK version 2020.1 (and earlier) is affected by a stack-based buffer overflow vulnerability potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file.</td></tr>
<tr><td>5</td><td>CVE-2021-39817</td><td>119</td><td></td><td>Exec Code Overflow Mem. Corr.</td><td>2021-09-01</td><td>2021-09-08</td><td>9.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.</td></tr>
<tr><td>6</td><td>CVE-2021-39816</td><td>119</td><td></td><td>Exec Code Overflow Mem. Corr.</td><td>2021-09-01</td><td>2021-09-08</td><td>9.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.</td></tr>
<tr><td>7</td><td>CVE-2021-39615</td><td>798</td><td></td><td></td><td>2021-08-23</td><td>2021-08-30</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">** UNSUPPORTED WHEN ASSIGNED ** D-Link DSR-500N version 1.02 contains hard-coded credentials for undocumented user accounts in the '/etc/passwd' file.If an attacker succeeds in recovering the cleartext password of the identified hash value, he will be able to log in via SSH or Telnet and thus gain access to the underlying embedded Linux operating system on the device. Fixed in version 2.12/2. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.</td></tr>
<tr><td>8</td><td>CVE-2021-39608</td><td>434</td><td></td><td>Exec Code</td><td>2021-08-23</td><td>2021-09-14</td><td>9.0</td><td>None</td><td>Remote</td><td>Low</td><td>???</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">Remote Code Execution (RCE) vulnerabilty exists in FlatCore-CMS 2.0.7 via the upload addon plugin, which could let a remote malicious user exeuct arbitrary php code.</td></tr>
<tr><td>9</td><td>CVE-2021-39279</td><td>78</td><td></td><td></td><td>2021-09-07</td><td>2021-09-09</td><td>9.0</td><td>None</td><td>Remote</td><td>Low</td><td>???</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7,</td></tr>
</table>

*647 vulnerabilidades

CRÍTICAS

Fonte:https://www.cvedetails.com/vulnerability-list.php?vendor_id=0&product_id=0&version_id=0&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=9&cvssscoremax=10&year=0&month=0&cweid=0&order=1&trc=18757&sha=c560d509f935c26128bfb13d2f2dadfcea62215b
*Setembro

Principais Vulnerabilidades no mundo em 2020



HELPNETSECURITY

TOP 10 MOST EXPLOITED VULNERABILITIES FROM 2020

1. CVE-2020-0796: Windows SMBv3 Client/Server Remote Code Execution Vulnerability (codename: *SMBGhost*)

2. CVE-2020-5902: F5 Networks BIG-IP TMUI RCE vulnerability

3. CVE-2020-1472: Microsoft Netlogon Elevation of Privilege (codename: *Zerologon*)

4. CVE-2020-0601: Windows CryptoAPI Spoofing Vulnerability (codename: *CurveBall*)

5. CVE-2020-14882: Oracle WebLogic Server RCE

6. CVE-2020-1938: Apache Tomcat AJP File Read/Inclusion Vulnerability (codename: *GhostCat*)

7. CVE-2020-3452: Cisco ASA and Firepower Path Traversal Vulnerability

8. CVE-2020-0688: Microsoft Exchange Server Static Key Flaw Could Lead to Remote Code Execution

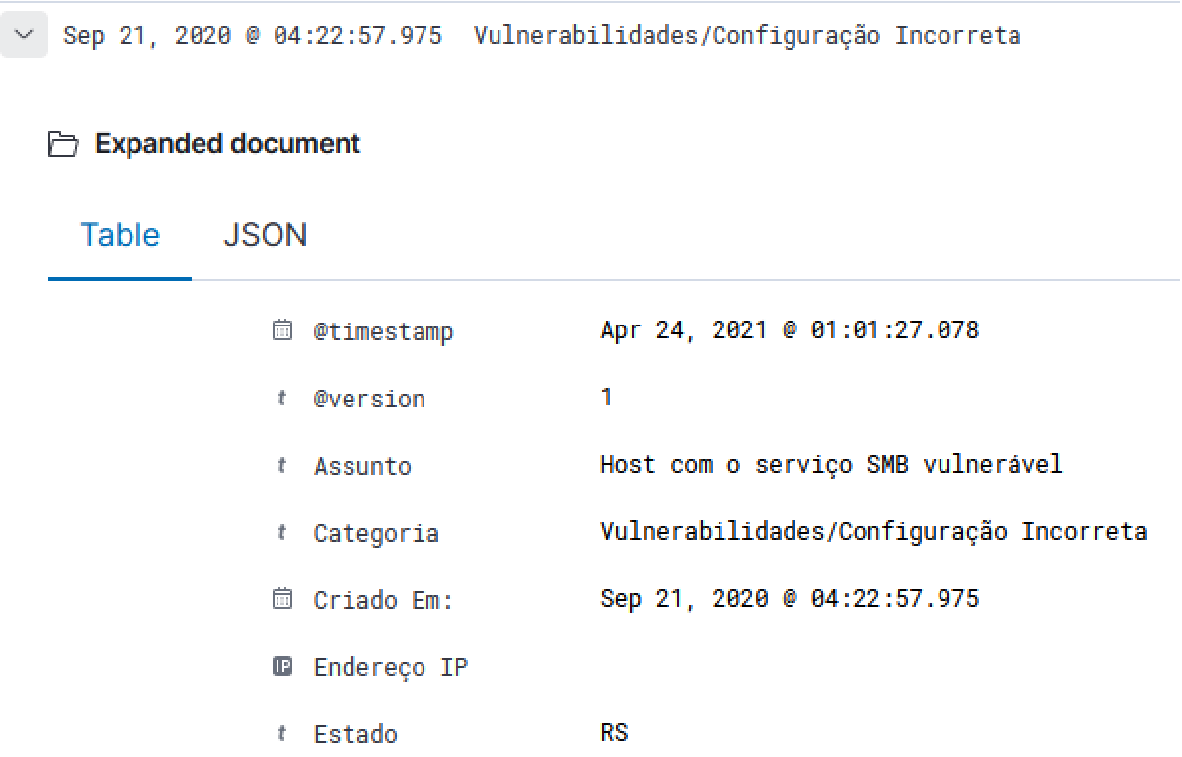
9. CVE-2020-16898: Windows TCP/IP Vulnerability (codename: *Bad Neighbor*)

10. CVE-2020-1350: Critical Windows DNS Server RCE (codename: *SIGRed*)

SOURCE: vFeed

E se eu não tratar uma vulnerabilidade ?

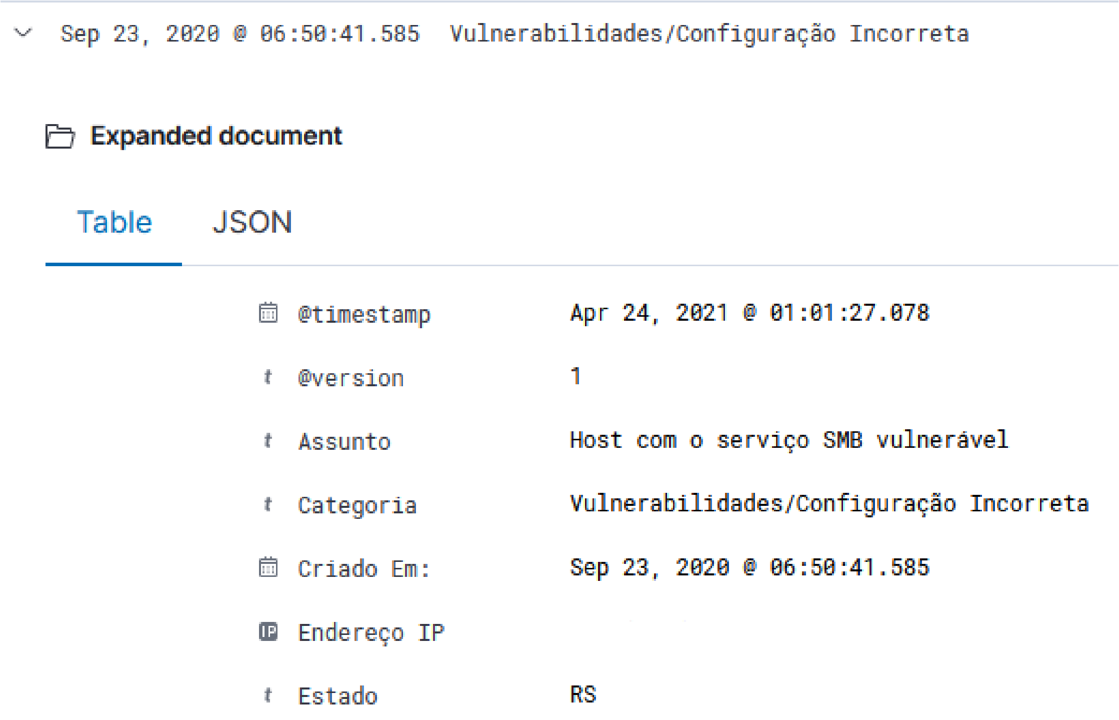
Vulnerabilidades -> Incidentes nos clientes RNP



Sep 21, 2020 @ 04:22:57.975 Vulnerabilidades/Configuração Incorreta

Expanded document

@timestamp	Apr 24, 2021 @ 01:01:27.078
@version	1
Assunto	Host com o serviço SMB vulnerável
Categoria	Vulnerabilidades/Configuração Incorreta
Criado Em:	Sep 21, 2020 @ 04:22:57.975
Endereço IP	
Estado	RS

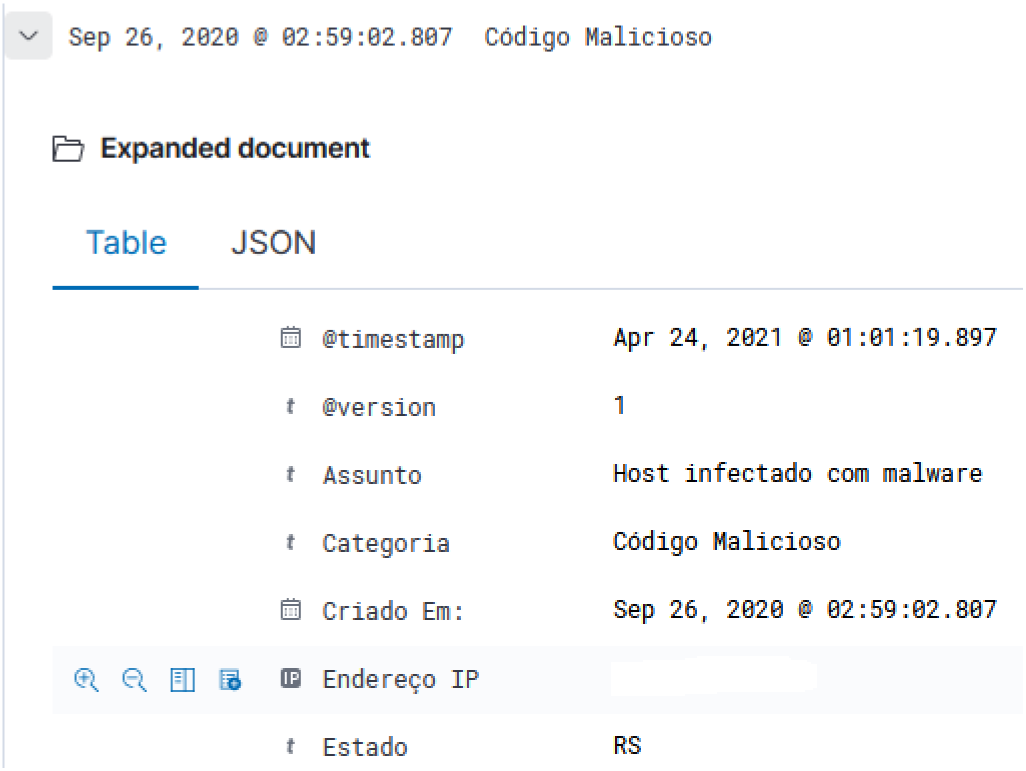


Sep 23, 2020 @ 06:50:41.585 Vulnerabilidades/Configuração Incorreta

Expanded document

@timestamp	Apr 24, 2021 @ 01:01:27.078
@version	1
Assunto	Host com o serviço SMB vulnerável
Categoria	Vulnerabilidades/Configuração Incorreta
Criado Em:	Sep 23, 2020 @ 06:50:41.585
Endereço IP	
Estado	RS

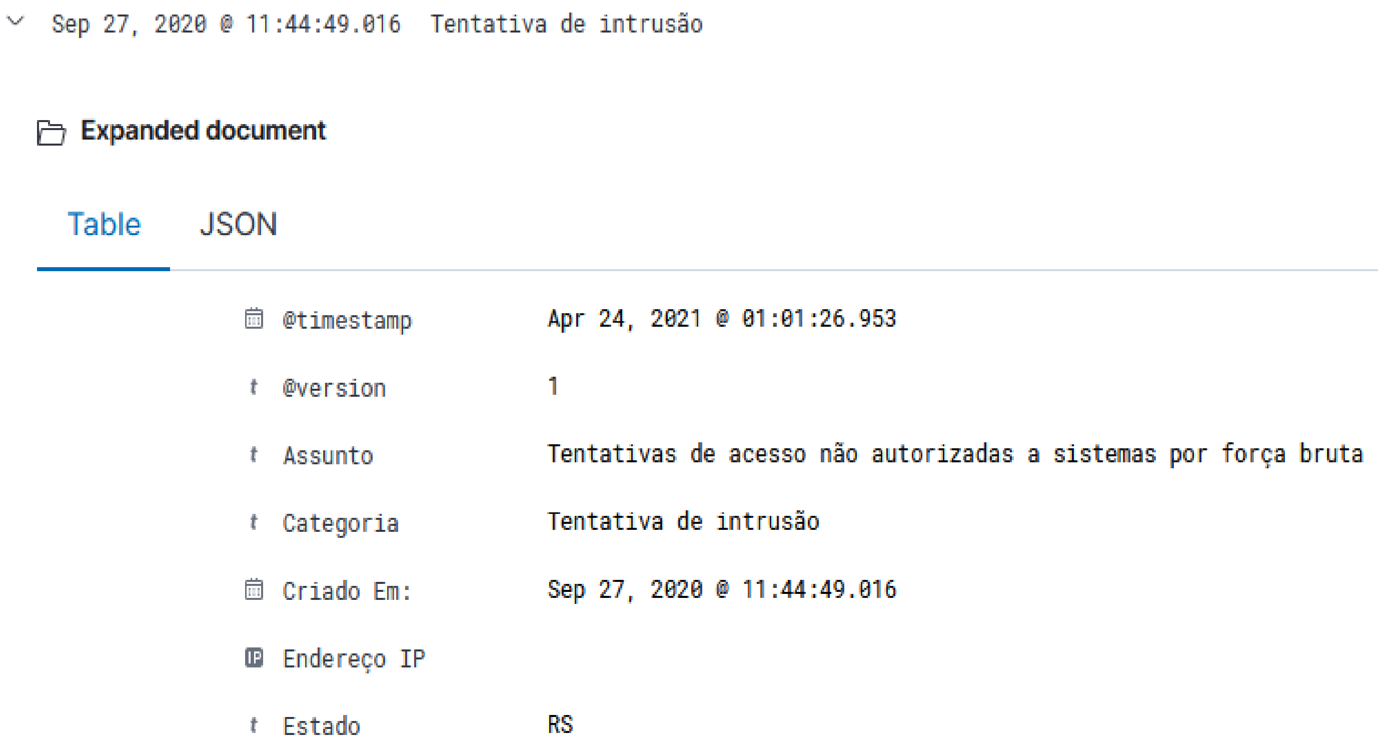
Vulnerabilidades -> Incidentes nos clientes RNP



Sep 26, 2020 @ 02:59:02.807 Código Malicioso

Expanded document

@timestamp	Apr 24, 2021 @ 01:01:19.897
@version	1
Assunto	Host infectado com malware
Categoria	Código Malicioso
Criado Em:	Sep 26, 2020 @ 02:59:02.807
Endereço IP	[redacted]
Estado	RS



Sep 27, 2020 @ 11:44:49.016 Tentativa de intrusão

Expanded document

@timestamp	Apr 24, 2021 @ 01:01:26.953
@version	1
Assunto	Tentativas de acesso não autorizadas a sistemas por força bruta
Categoria	Tentativa de intrusão
Criado Em:	Sep 27, 2020 @ 11:44:49.016
Endereço IP	
Estado	RS

Porque é melhor tratar uma vulnerabilidade e não um incidente ?

It costs three times more to clean up an incident than to prevent one

Fonte: Tenable
https://pt-br.tenable.com/blog/the-cost-of-incident-response?tns_redirect=true

Travelex Bank

HONDA
ASAS DA LIBERDADE

THE UNIVERSITY OF UTAH

STJ
SUPERIOR
TRIBUNAL DE JUSTIÇA

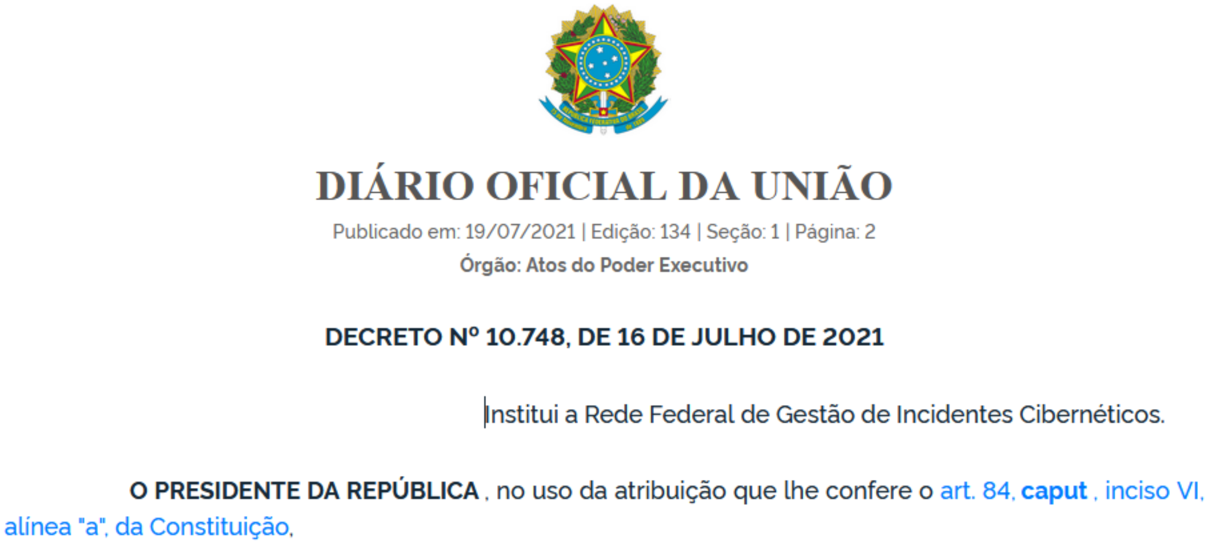
Como se proteger de incidentes de segurança da informação ?

Processo de Gestão de vulnerabilidades;

Processo de Gestão de Incidentes;

Monitoramento efetivo de recursos;

Hardening dos serviços utilizados.



DIÁRIO OFICIAL DA UNIÃO

Publicado em: 19/07/2021 | Edição: 134 | Seção: 1 | Página: 2

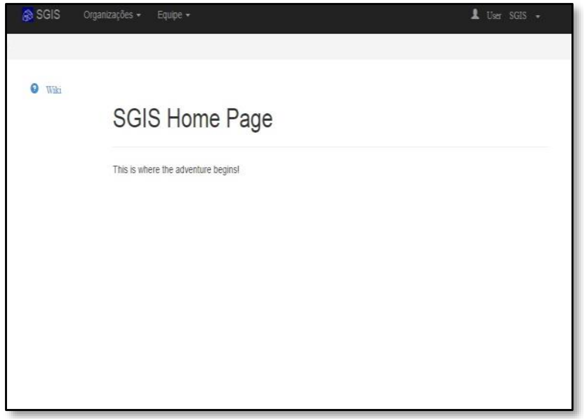
Órgão: Atos do Poder Executivo

DECRETO Nº 10.748, DE 16 DE JULHO DE 2021

Institui a Rede Federal de Gestão de Incidentes Cibernéticos.

O PRESIDENTE DA REPÚBLICA , no uso da atribuição que lhe confere o art. 84, **caput** , inciso VI, alínea "a", da Constituição,

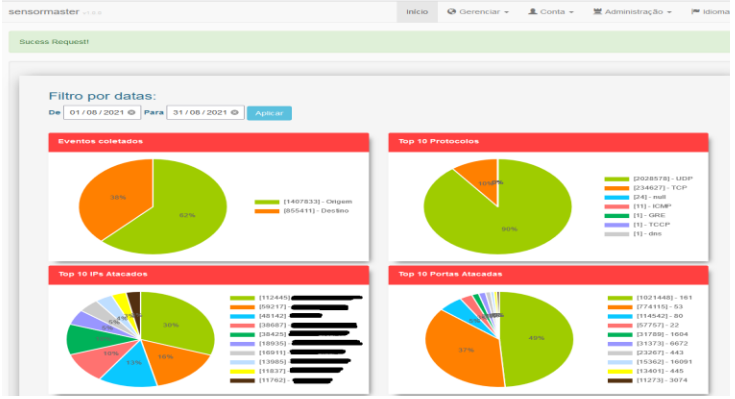
Como a RNP pode te ajudar ?


SGIS · Organizações · Equipe · User · SGIS

Wiki

SGIS Home Page

This is where the adventure begins!


sensormaster · Início · Gerenciar · Conta · Administração · Idioma

Sucess Request!

Filtro por datas:

De 01 / 08 / 2021 Para 31 / 08 / 2021 Aplicar

Eventos coletados

[1407833] - Origem
[855411] - Destino

Top 10 Protocolos

[2028578] - UDP
[234627] - TCP
[24] - null
[11] - ICMP
[1] - GRE
[1] - TCCP
[1] - dns

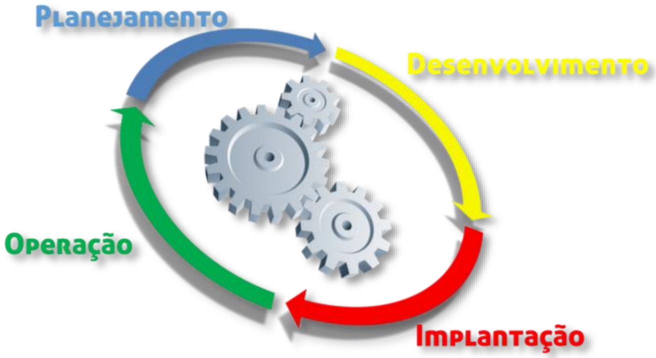
Top 10 IPs Atacados

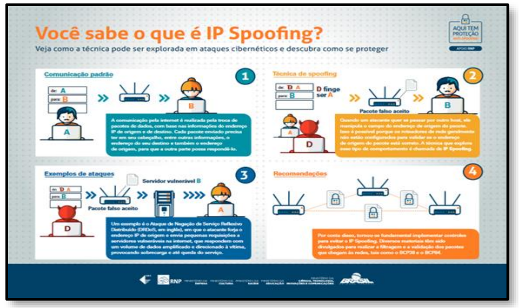
[112445] - [redacted]
[59217] - [redacted]
[48142] - [redacted]
[38687] - [redacted]
[38425] - [redacted]
[18935] - [redacted]
[16911] - [redacted]
[13985] - [redacted]
[11837] - [redacted]
[11762] - [redacted]

Top 10 Portas Atacadas

[1021448] - 161
[774115] - 53
[114542] - 80
[57757] - 22
[31789] - 1604
[31373] - 6672
[23267] - 443
[15362] - 16091
[13401] - 445
[11273] - 3074

Estabelecimento de CSIRTs




Você sabe o que é IP Spoofing?

Veja como a técnica pode ser explorada em ataques cibernéticos e descubra como se proteger

AQUI TEM PROTEÇÃO
APOIO RNP

1 Comunicação padrão

de: A
para: B
A
B

A comunicação pela internet é realizada pela troca de pacotes de dados, com base nas informações do endereço IP de origem e de destino. Cada pacote enviado precisa ter em seu cabeçalho, entre outras informações, o endereço do seu destino e também o endereço de origem, para que a outra parte possa respondê-lo.

2 Técnica de spoofing

Quando um atacante quer se passar por outro host, ele manipula o campo do endereço de origem do pacote. Isso é possível porque os roteadores de rede geralmente não estão configurados para validar se o endereço de origem do pacote está correto. A técnica que explora esse tipo de comportamento é chamado de IP Spoofing.

3 Exemplos de ataques

Um exemplo é o Ataque de Negação de Serviço Reflexivo Distribuído (DRDoS, em inglês), em que o atacante forja o endereço IP de origem e envia pequenas requisições a servidores vulneráveis na internet, que respondem com um volume de dados amplificado e direcionado à vítima, provocando sobrecarga e até queda do serviço.

4 Recomendações

Por conta disso, tornou-se fundamental implementar controles para evitar o IP Spoofing. Diversos materiais têm sido divulgados para realizar a filtragem e a validação dos pacotes que chegam às redes, tais como o BCP38 e o BCP84.

'21 DISI

DIA INTERNACIONAL DE SEGURANÇA EM INFORMÁTICA

SEGURANÇA DIGITAL COMEÇA CEDO

#DISI21

11FEV · 16h

Quinta-feira

PARTICIPE

Política de Privacidade

ESCOLA SUPERIOR DE REDES

webinar com

Roberto Lauretti

Marcello Zillo Neto

É amanhã!

WEBINAR: Criando e mantendo um software seguro.

Episódio 5: Criando uma infraestrutura minimamente segura em cloud

13/08/21 às 10h

inscreva-se

RNP
MINISTÉRIO DO TURISMO
MINISTÉRIO DA DEFESA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DAS COMUNICAÇÕES
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES
PÁTRIA AMADA BRASIL

Campanha Técnicas/Webinars/DISI

Projetos específicos

Obrigado!

Rildo Souza
rildo dot souza at rnp dot br

Telefone:
0800 722 0216

WTR
WORKSHOP
DE TECNOLOGIA DE REDES DO POP-RS
> 2021

APOIO

nic.br

REALIZAÇÃO

PoP-RS
Ponto de Presença da
RNP no Rio Grande do Sul

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

MINISTÉRIO DO
TURISMO

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DAS
COMUNICAÇÕES

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÕES

PÁTRIA AMADA
BRASIL
GOVERNO FEDERAL