Governo do Estado de
RONDÔNIA
SETIC

Coordenadoria Segurança da Informação RELATÓRIO MENSAL Junho/2021

2021

GOVERNO DO ESTADO DE RONDÔNIA
SUPERINTENDÊNCIA ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
DIRETORIA TÉCNICA

Relatório Mensal - Junho/2021

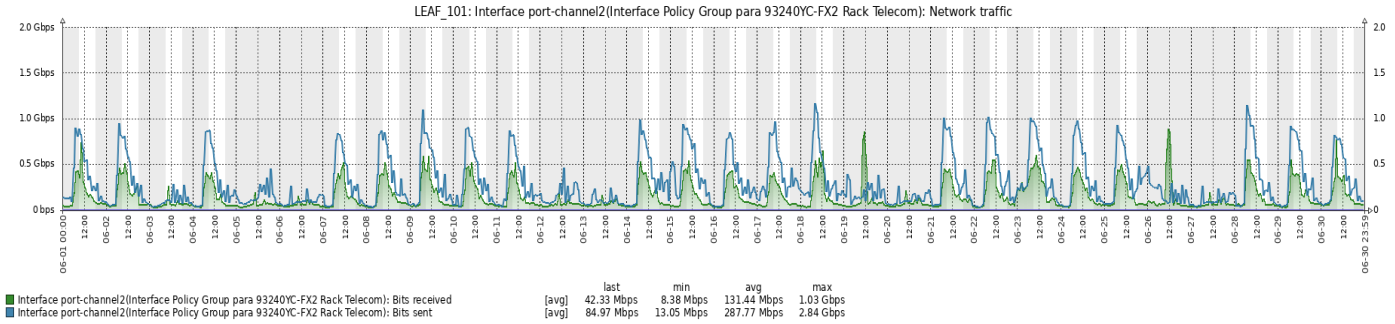
Sumário

1. Introdução

Está Coordenadoria de Segurança, elaborou este relatório como fins de apresentação de aumento de utilização dos serviços como Redes, Ataques e Vulnerabilidade no mês de Junho.

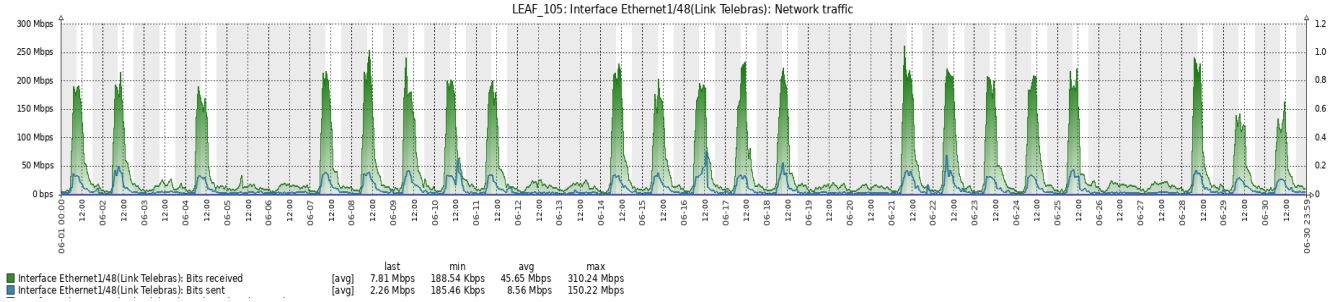
2. Tráfego de Rede

Considerando os dados de tráfego de rede transferidos via Cores de Comunicação de Dados da SETIC, entre estações de trabalho do Palácio Rio Madeira, INFOVIA e serviços hospedados, aferimos o Volume Total de **140 TB** de informação trafegada no mês deste relatório.

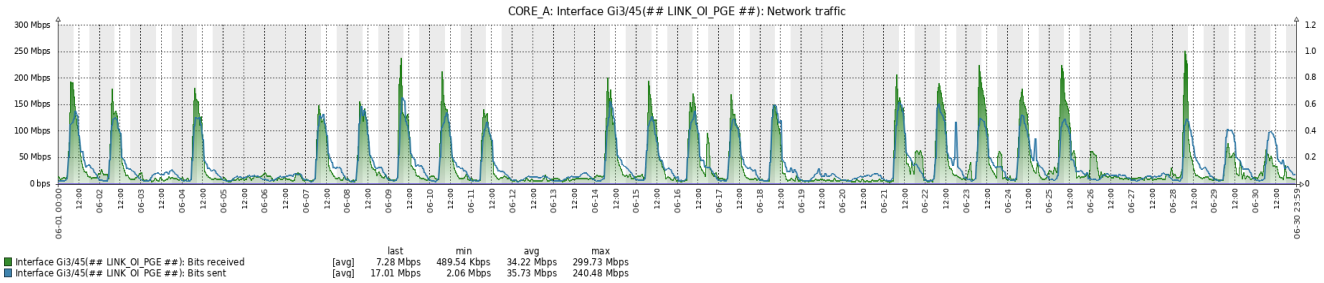


Monitoramento de tráfego Cores SETIC

Além disso, foram consumidos **41 TB** de tráfego da Internet, considerando acesso dos usuários a aplicações de Governo expostas na Internet e acesso a serviços pelo público geral.



Monitoramento de tráfego Cores Link Telebrás



Monitoramento de tráfego Cores Link Oi

2.1 Consumo por Secretária

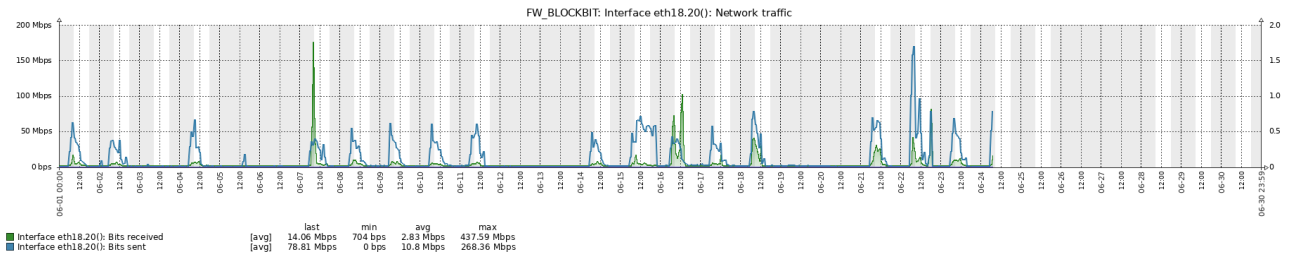
Considerando os dados de tráfego de rede transferidos via Cores de Comunicação de Dados da SETIC, entre estações de trabalho do Palácio Rio Madeira, INFOVIA e serviços hospedados, aferimos o Volume Total de **11,7 TB** de informação trafegada no mês deste relatório por secretaria.

Os dados referem-se às três maiores consumidoras deste mês de Junho.

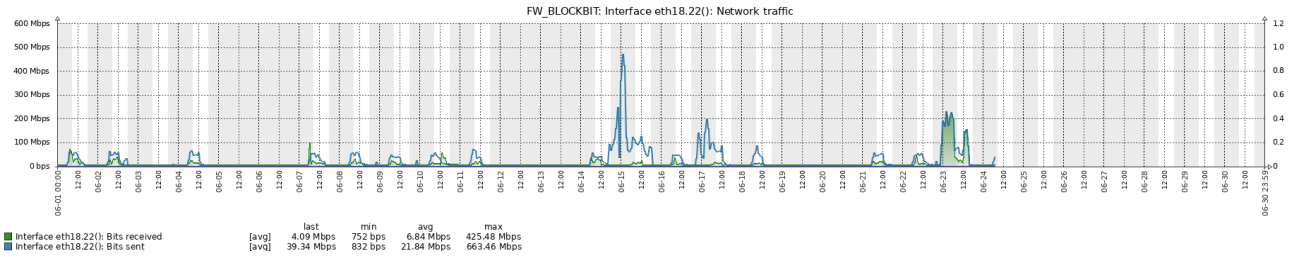
Secretária DER/SEOSP: **4 TB**

Secretária SUGESP: **9 TB**

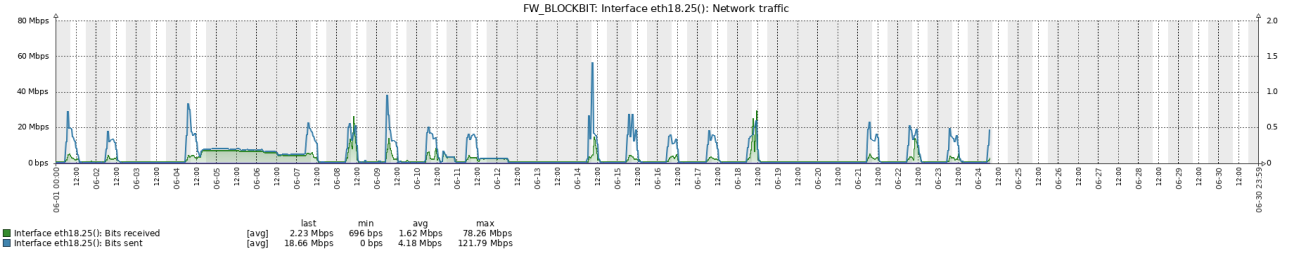
Secretária SEAGRI: **1 TB**



Monitoramento de tráfego DER/SEOSP



Monitoramento de tráfego SUGESP



Monitoramento de tráfego SEAGRI

3. Ataques

Vale à pena frisar que ainda não possuímos uma infraestrutura que nos garanta a segurança de dados, no que tange às tecnologias de proteção topo de linha no mercado de TI. Por este motivo no mês de **Junho**, a estatística de tentativas de intrusão, para o melhor funcionamento da rede, o serviço foi desabilitado, pois devido alta demanda de consumo, o equipamento disponível não suporta o recurso em nosso ambiente.

4. Vulnerabilidades

Trata-se das reanálises de vulnerabilidades realizadas sem servidores de rede pertencentes ao Governo do Estado de Rondônia gerenciados ou hospedados pela SETIC, utilizando-se os softwares Nmap 1 e OpenVAS 2.

Tais procedimentos se deram em decorrência das diretrizes da Coordenação de Segurança da Informação da SETIC, bem como a solicitação da equipe de Data Center da Coordenação de Infraestrutura da SETIC.

O OpenVAS, ao analisar determinado alvo, classifica as vulnerabilidades encontradas em 3 (três) diferentes níveis de gravidade: **alto, médio e baixo**. Destaca-se ainda que apresenta também o nível denominado “log”, que objetiva trazer informações sobre o alvo, não sendo objeto de discussão neste relatório.

Ao todo, foram reanalisados **53** (cinquenta e três) servidores de rede, dos quais **10 (18,9%)** apresentaram **alto** nível de gravidade, **27 (50,9%)** apresentaram **médio** nível, **0 (0%)** apresentaram **baixo** nível, conforme classificação do OpenVAS, destacando-se ainda que **7 (13,2%)** servidores não apresentaram **nenhuma** vulnerabilidade.

Também encontramos **9 (17%)** endereços que não responderam, ou desligados ou inalcançáveis.

Importante ressaltar que nas análises, alguns servidores que apresentaram alto nível de gravidade também apresentaram gravidades de nível médio e baixo, bem como alguns servidores que apresentaram médio nível de gravidade também apresentaram gravidades de nível baixo.

No decorrer das análises o OpenVAS detectou **1133 notificações**, sendo que cada uma dessas representa uma vulnerabilidade. Dentre as notificações apresentadas destacam-se: **181 (16%)** de **alto** nível, **898 (79,3%)** de **médio** nível e **54 (4,8%)** de **baixo** nível.

Nos testes realizados foram identificadas diversas vulnerabilidades, entretanto não se descarta outras que por ventura não foram detectadas ou que surjam futuramente.

4.1 CONTEXTO DA ANÁLISE DE VULNERABILIDADES

Considerando as novas diretrizes da Coordenação de Segurança da Informação da SETIC, a solicitação da equipe de Data Center da Coordenação de Infraestrutura da SETIC, realizou-se as análises nos seguintes hosts:

10.11.19.63 - 10.11.3.49 - 10.39.30.2 - 10.40.35.254 - 10.50.0.149 - 10.50.0.168 - 10.50.0.201 - 10.50.0.43 - 10.50.0.62 - 10.50.0.65 - 10.50.0.84 - 10.9.0.5 - 10.9.0.7 - 10.9.0.8 - 10.9.16.52 - 10.9.9.173 - 10.9.9.175 - 131.72.154.180 - 172.16.0.103 - 172.16.0.105 - 172.16.0.110 - 172.16.0.113 - 172.16.0.114 - 172.16.0.115 - 172.16.0.117 172.16.0.120 - 172.16.0.121 - 172.16.0.122 - 172.16.0.123 - 172.16.0.130 - 172.16.0.133 - 172.16.0.134 - 172.16.0.135 - 172.16.0.136 - 172.16.0.137 - 172.16.0.143 - 172.16.0.145 - 172.16.0.150 - 172.16.0.153 - 172.16.0.157 - 172.16.0.158 - 172.16.0.159 - 172.16.0.160 - 172.16.0.161 - 172.16.0.162 - 172.16.0.164 - 172.16.0.165 - 172.16.0.166 - 172.16.0.167 - 172.16.0.168 - 172.16.0.169 - 172.16.0.17 - 172.16.0.170

Nesse sentido, primeiro foi iniciada a etapa de levantamento de informações e versionamentos, utilizando-se o Nmap. Logo em seguida, utilizou-se um software de análise de vulnerabilidade genérico, OpenVAS.

4.2 GRÁFICOS

Utilizando-se do OpenVAS, considerando sua classificação das vulnerabilidades em 3 (três) diferentes níveis de gravidade (**alto, médio e baixo**) foi possível re-analisar **53** (cinquenta e três) servidores de rede, dos quais **10 (18,9%)** apresentaram **alto** nível de gravidade, **27 (50,9%)** apresentaram **médio** nível, **0 (0%)** apresentaram **baixo** nível, conforme classificação do OpenVAS, destacando-se ainda que **7 (13,2%)** servidores não apresentaram **nenhuma** vulnerabilidade, também encontramos **9 (17%)** endereços que não responderam, ou desligados ou inalcançáveis, conforme “Gráfico 1 – Nível de gravidade” abaixo:

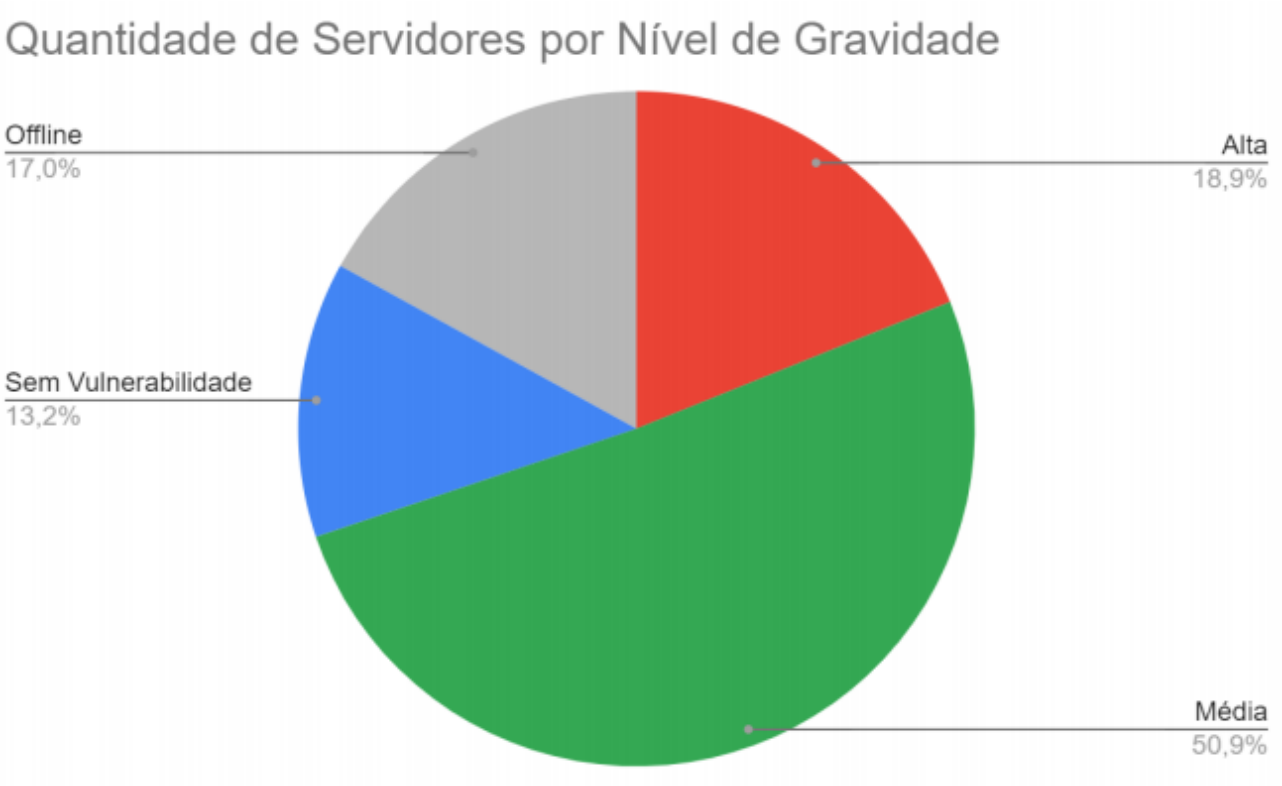


Gráfico 1 – Quantidade de Servidores

No que diz respeito às notificações apresentadas pelo OpenVAS, destacam-se que foram detectadas **181 (16%)** de **alto** nível, **898 (79,3%)** de **médio** nível e **54 (4,8%)** de **baixo** nível, conforme “Gráfico 2 – Total de notificações” abaixo:

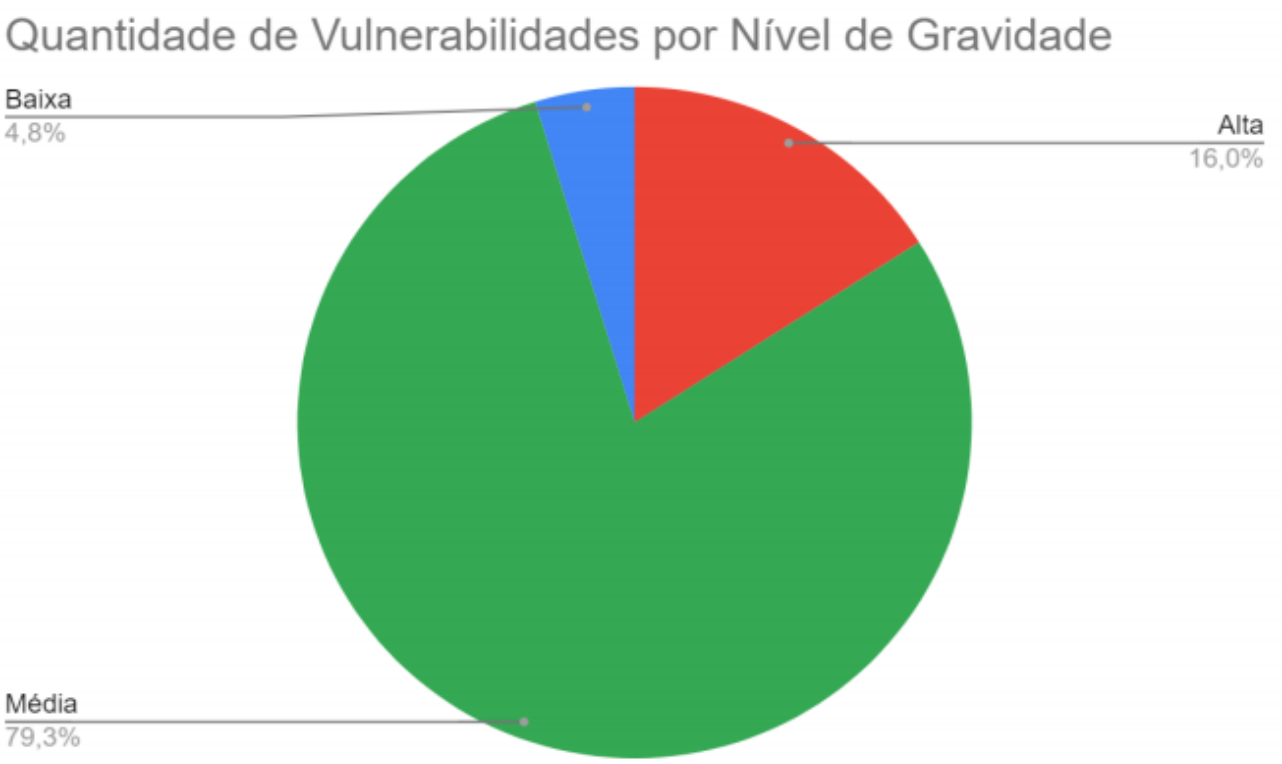


Gráfico 2 – Quantidade de Vulnerabilidade

Além disso, com base nos relatórios do OpenVAS, procurou-se categorizar as principais vulnerabilidades encontradas nos servidores de rede que foram analisados, criando as seguintes categorias: Web (PHP, HTTP, APACHE), Chaves de Segurança (SSL, TLS, OPENSSH), Acesso Remoto (RPC, FTP, DCE, TCP), Informações do Sistema (TCP TIMESTAMPS), Compartilhamento de Arquivos (Backup, SMB), Banco de Dados (MariaDB, SQL), Sistemas e Aplicações.

Dessa forma, procurou-se destacar a vulnerabilidade mais crítica de cada servidor e classificá-la em uma dessas categorias, com objetivo de facilitar a identificação do segmento que se encontra mais vulnerável na rede, exigindo atenção e adoção de políticas de correção e mitigação de falhas e problemas de segurança. Sendo assim, foi possível perceber que a maioria das vulnerabilidades encontradas estão vinculadas à Acesso Remoto (26 servidores) Chaves de Segurança (37 servidores) e Informações do Sistema (27 servidores), conforme observado no “Gráfico 3 – Categorias de vulnerabilidades” abaixo:

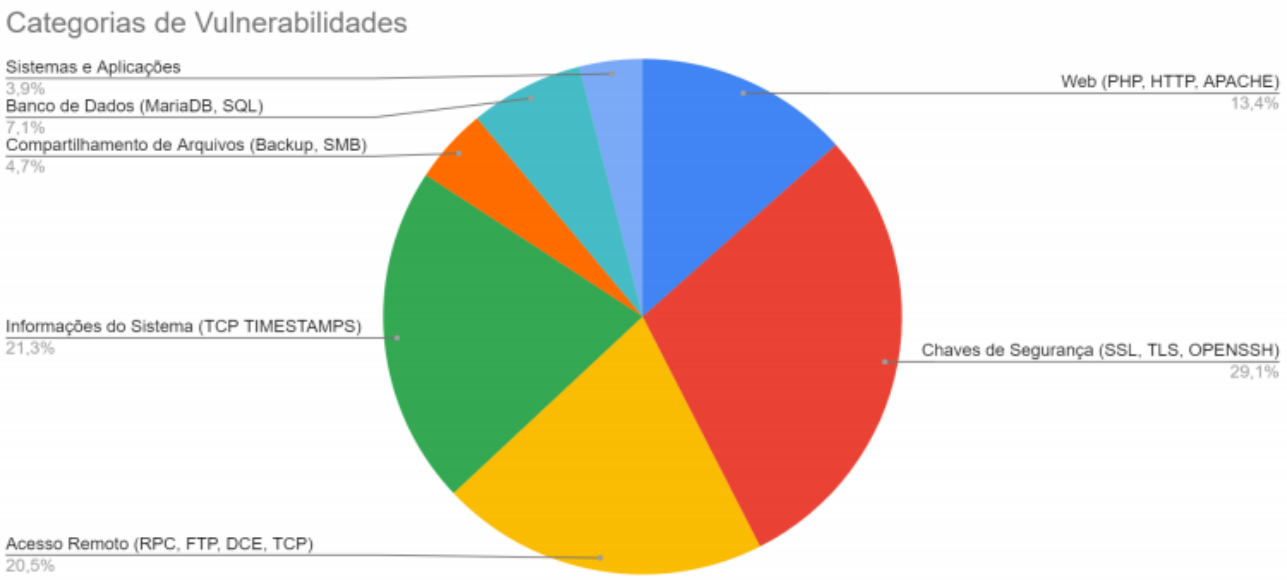


Gráfico 3 – Categorias de Vulnerabilidade

4.3 AÇÕES CORRETIVAS

Após a realização das análises e produção dos relatórios, contendo informações conjuntas do Nmap e OpenVAS, estes foram enviados ao setor de Data Center, responsável por realizar as correções aplicando as medidas necessárias. Tal procedimento foi determinado pela Coordenação de Segurança da Informação da SETIC, considerando que esse setor que administra os servidores que foram analisados.

Os relatórios foram enviados por meio de chamados abertos pelo GLPI (https://atendimento.detic.ro.gov.br/), sistema de controle de requisições da SETIC, sob os protocolos de número:

2021041138 - 2021085339 - 2021085342 - 2021085344 - 2021085347 - 2021085350 - 2021085352 - 2021085856 - 2021085356 - 2021085359 - 2021085365 - 2021085887 -

2021085889 - 2021085890 - 2021085891 - 2021085893 - 2021085895 - 2021085907 - 2021085908 - 2021085909 - 2021085910 - 2021085911 - 2021085913 - 2021085914 - 2021085916 - 2021086257 - 2021086261 - 2021086267 - 2021086273 - 2021086278 - 2021086282 - 2021086285 - 2021086289 - 2021086293 - 2021086296 - 2021086958 - 2021086961 - 2021086962 - 2021086963 - 2021086964 - 2021086967 - 2021086968 2021086971 - 2021086972

No APÊNDICE – Controle de análises, encontra-se uma tabela contendo informações sobre as referências, endereços de IP, datas das análises, softwares utilizados para realizá-las, nível de gravidade, as principais falhas detectadas, a vinculação de endereços internos ou externos quando identificados, o número do chamado no GLPI e sua data de abertura.

APÊNDICE – Controle de análises

IP	Num. Chamado (GLPI)	Data Chamado (GLPI)	Solução apresentada no chamado	Data da Reanálise	Softwares Utilizados	√Gravidade			Principal Gravidade	Principais Falhas	Num. Chamado (GLPI)	Data Chamado (GLPI)
10.11.19.63	2020071872	17/7/2020 12:36	Estou cientes das vulnerabilidades e ire	10/6/2021	NMAP e OPENVAS.	15	28	5	Alta	OS End Of Life Detection / Postgre	2021041138	10-06-2021 10:48
10.11.3.49	2020093263	25/9/2020 09:33	Solução aprovada * Patrick Hebert Da S	10/6/2021	NMAP e OPENVAS.	0	2	1	Média	Missing 'httpOnly' / DCE-RPC / T	2021085339	10-06-2021 10:37
10.39.80.2	2020081080	7/8/2020 10:32	sem posicionamento sobre						-			
10.40.35.254	2020093524	29/9/2020 07:59	Apontamento apenas interno. * Gabriel Carrijo Bento Teixeira						-			
10.50.0.149	2020111469	10/11/2020 11:39	* Ederson Vanazzi Alves	10/6/2021	NMAP e OPENVAS.	0	2	0	Média	DCE-RPC / SSL-TLS	2021085342	10-06-2021 10:43
10.50.0.168	2021010689	12/1/2021 10:42	sem posicionamento sobre	10/6/2021	NMAP e OPENVAS.	0	2	0	Média	DCE-RPC / SSL-TLS	2021085344	10-06-2021 10:52
10.50.0.201	2021010962	14/1/2021 13:12	sem posicionamento sobre	10/6/2021	NMAP e OPENVAS.	0	2	0	Média	DCE-RPC / SSL-TLS	2021085347	10-06-2021 10:55
10.50.0.48	2021010689	12/1/2021 10:42	sem posicionamento sobre						-			
10.50.0.62	2021040835	15/4/2021 09:43	Aplicando correções. * Ederson Vanazz	10/6/2021	NMAP e OPENVAS.	0	2	0	Média	DCE-RPC / SSL-TLS	2021085350	10-06-2021 10:59
10.50.0.65	2020091179	9/9/2020 10:00	VM de teste DETIC, sera encerrado o chamado e desabilitada a maquina virtual. * Ederson Vanazzi Alves						-			
10.50.0.84	2021040832	15/4/2021 09:41	Aplicando correção * Ederson Vanazzi	10/6/2021	NMAP e OPENVAS.	0	4	1	Média	DCE-RPC / SSL-TLS / TCP timestam	2021085352	10-06-2021 11:04
10.9.0.5	2021040699	14/4/2021 07:22	sem posicionamento sobre	10/6/2021	NMAP e OPENVAS.	0	380	1	Média	Backup File Scanner / Missing 'htt	2021085856	17-06-2021 09:44
10.9.0.7	2021040640	13/4/2021 09:25	sem posicionamento sobre	10/6/2021	NMAP e OPENVAS.	0	19	1	Média	Backup File Scanner / Missing 'htt	2021085356	10-06-2021 11:07
10.9.0.8	2021040346	8/4/2021 09:44	Aplicando correções. o TimeStamp não f	10/6/2021	NMAP e OPENVAS.	0	2	0	Média	OpenSSH / SSL-TLS	2021085359	10-06-2021 11:10
10.9.16.52	2021021004	9/2/2021 11:06	Correções realizadas. * Ramisses Evang	10/6/2021	NMAP e OPENVAS.	0	0	0			2021085365	10-06-2021 11:13
10.9.9.173	2021040349	8/4/2021 09:48	Verificando, VM sera descontinuada. * Ederson Vanazzi Alves						-			
10.9.9.175	2021040348	8/4/2021 09:46	Verificando, VM sera descontinuada. * Ederson Vanazzi Alves						-			
131.72.154.180	2021030770	9/3/2021 13:00	* Ramisses Evangelista Araújo						-			
172.16.0.103	2021021517	16/2/2021 08:17	sem posicionamento sobre	17/6/2021	NMAP e OPENVAS.	0	7	1	Média	Microsoft SQL Server / SSL/TLS / D	2021085887	17-06-2021 12:01
172.16.0.105	2021031936	25/3/2021 09:43	sem posicionamento sobre	17/6/2021	NMAP e OPENVAS.	0	5	1	Média	OpenSSH / SSH Weak Encryption A	2021085889	17-06-2021 12:07
172.16.0.110	2021031730	23/3/2021 08:30	As seguintes correções foram executada	17/6/2021	NMAP e OPENVAS.	0	3	1	Média	DCE-RPC / SSL-TLS / TCP timestam	2021085890	17-06-2021 12:11
172.16.0.113	2020081740	12/8/2020 11:21	Aplicada atualização corretiva * Ederso	17/6/2021	NMAP e OPENVAS.	1	4	1	Alta	OpenSSH / TCP timestamps	2021085891	17-06-2021 12:14
172.16.0.114	2021031937	25/3/2021 09:45	O Sr. Jairo Cunha (SETIC), esta em fase	17/6/2021	NMAP e OPENVAS.	0	2	0	Média	DCE-RPC / SSL-TLS	2021085893	17-06-2021 12:18
172.16.0.115	2021031939	25/3/2021 09:47	Em conversa na data de hj (08/04/2021), com o Sr. David Bremide, o mesmo me informou que em conver						-			
172.16.0.117	2021032177	30/3/2021 08:45	sem posicionamento sobre	17/6/2021	NMAP e OPENVAS.	3	37	2	Alta	PHP End Of Life Detection / Apach	2021085895	17-06-2021 12:22
172.16.0.120	2021030422	4/3/2021 09:44	Verificado junto com o Analista Tiago Sil	17/6/2021	NMAP e OPENVAS.	0	4	0	Média	Microsoft SQL Server / SSL/TLS /	2021085907	17-06-2021 12:26
172.16.0.121	2021030423	4/3/2021 09:46	VM encontra-se obsoleta e desligada. *	17/6/2021	NMAP e OPENVAS.	0	1	1	Média	DCE-RPC / TCP timestamps	2021085908	17-06-2021 12:28
172.16.0.122	2020082277	17/8/2020 09:04	Verificando com equipe de desenvolvime	17/6/2021	NMAP e OPENVAS.	45	67	6	Alta	PHP End Of Life Detection / Apach	2021085909	17-06-2021 12:31
172.16.0.123	2021040351	8/4/2021 09:52	Aplicando correções. * Ederson Vanazz	17/6/2021	NMAP e OPENVAS.	0	3	1	Média	DCE-RPC / SSL-TLS / TCP timestam	2021085910	17-06-2021 12:34
172.16.0.130	2021021514	16/2/2021 08:13	sem posicionamento sobre	17/6/2021	NMAP e OPENVAS.	0	6	1	Média	Microsoft SQL Server / SSL/TLS / D	2021085911	17-06-2021 12:37
172.16.0.133	2021021180	11/2/2021 09:14	Servidor esta sendo usado como consulta	17/6/2021	NMAP e OPENVAS.	91	167	13	Alta	PHP End Of Life Detection / OpenS	2021085913	17-06-2021 12:39
172.16.0.134	2021021183	11/2/2021 09:19	Correções realizadas. * Ramisses Evang	17/6/2021	NMAP e OPENVAS.	0	0	0			2021085914	17-06-2021 12:42
172.16.0.135	2021021516	16/2/2021 08:15	sem posicionamento sobre	17/6/2021	NMAP e OPENVAS.	0	6	1	Média	Microsoft SQL Server / SSL/TLS / D	2021085916	17-06-2021 12:44
172.16.0.136	2021040354	8/4/2021 09:55	Entrando em contado com o pessoal do	22/6/2021	NMAP e OPENVAS.	0	5	1	Média	DCE-RPC / SSL-TLS / TCP timestam	2021086257	22-06-2021 10:06

IP	Num. Chamado (GLPI)	Data Chamado (GLPI)	Solução apresentada no chamado	Data da Reanálise	Softwares Utilizados	√Gravidade			Principal Gravidade	Principais Falhas	Num. Chamado (GLPI)	Data Chamado (GLPI)
172.16.0.137	2021031292	17/3/2021 08:21	As seguinte correções foram efetuadas:	22/6/2021	NMAP e OPENVAS.	0	3	1	Média	DCE-RPC / SSL-TLS / TCP timestam	2021086261	22-06-2021 10:09
172.16.0.143	2020082569	18/8/2020 13:23	sem posicionamento sobre	22/6/2021	NMAP e OPENVAS.	13	76	6	Alta	Oracle MySQL Multiple Unspecifie	2021086267	22-06-2021 10:12
172.16.0.145	2021031493	19/3/2021 07:50	As seguintes vulnerabilidades foram cor	22/6/2021	NMAP e OPENVAS.	0	3	1	Média	DCE-RPC / SSL-TLS / TCP timestam	2021086273	22-06-2021 10:15
172.16.0.150	2020091537	10/9/2020 17:01	sem posicionamento sobre	22/6/2021	NMAP e OPENVAS.	6	27	1	Alta	MortBay / Eclipse Jetty End of Life	2021086278	22-06-2021 10:18
172.16.0.153	2020091525	10/9/2020 14:41	VM foi desligada e marcada como desc	22/6/2021	NMAP e OPENVAS.	3	4	1	Alta	OpenSSH Multiple Vulnerabilities A	2021086282	22-06-2021 10:21
172.16.0.157	2021031291	17/3/2021 08:20	As seguintes vulnerabilidades foram cor	22/6/2021	NMAP e OPENVAS.	0	3	1	Média	DCE-RPC / SSL-TLS / TCP timestam	2021086285	22-06-2021 10:23
172.16.0.158	2021030738	9/3/2021 10:20	Correções realizadas. * Ramisses Evang	22/6/2021	NMAP e OPENVAS.	0	0	0			2021086289	22-06-2021 10:25
172.16.0.159	2021030739	9/3/2021 10:22	Correções realizadas. * Ramisses Evang	22/6/2021	NMAP e OPENVAS.	0	0	0			2021086293	22-06-2021 10:27
172.16.0.160	2020091785	14/9/2020 10:45	* Ramisses Evangelista Araújo	22/6/2021	NMAP e OPENVAS.	0	0	0			2021086296	22-06-2021 10:30
172.16.0.161	2020081759	12/8/2020 12:02	Correção de vulnerabilidade 2.1.3 (Med	29/6/2021	NMAP e OPENVAS.	0	4	1	Média	DCE-RPC / SSL-TLS / TCP timestam	2021086958	29-06-2021 10:28
172.16.0.162	2021031286	17/3/2021 08:14	Verificando com equipe. * Ederson Van	29/6/2021	NMAP e OPENVAS.	3	5	1	Alta	HP Data Protector Multiple Vulner	2021086961	29-06-2021 10:31
172.16.0.164	2021031491	19/3/2021 07:46	Solução definitiva está sendo desenvolvi	29/6/2021	NMAP e OPENVAS.	0	2	0	Média	DCE-RPC / SSL-TLS	2021086962	29-06-2021 10:35
172.16.0.165	2021031948	25/3/2021 09:56	As seguintes correções foram aplicadas:	29/6/2021	NMAP e OPENVAS.				-			
172.16.0.166	2021031492	19/3/2021 07:48	Realizando update Nginx * Ederson Va	29/6/2021	NMAP e OPENVAS.	1	0	1	Alta	Nginx / TCP timestamps	2021086963	29-06-2021 10:38
172.16.0.167	2021030233	2/3/2021 11:46	sem posicionamento sobre	29/6/2021	NMAP e OPENVAS.	0	4	0	Média	Microsoft SQL Server 2016 / DCE-R	2021086964	29-06-2021 10:41
172.16.0.168	2021030231	2/3/2021 11:41	sem posicionamento sobre	29/6/2021	NMAP e OPENVAS.	0	4	0	Média	Microsoft SQL Server 2016 / DCE R	2021086967	29-06-2021 10:44
172.16.0.169	2021022074	23/2/2021 08:57	* Daltro Barbosa Filho	29/6/2021	NMAP e OPENVAS.	0	0	0			2021086968	29-06-2021 10:47
172.16.0.17	2021031946	25/3/2021 09:53	As seguintes correções de vulnerabilidad	29/6/2021	NMAP e OPENVAS.	0	3	1	Média	DCE-RPC / SSL-TLS / TCP timestam	2021086971	29-06-2021 10:52
172.16.0.170	2020091652	11/9/2020 12:34	* Ramisses Evangelista Araújo	29/6/2021	NMAP e OPENVAS.	0	0	0			2021086972	29-06-2021 10:56

Superintendência do
Estado para Resultados

Governo do Estado de
RONDÔNIA