Evandro Alves

CVE-2022-27255: Quando a CPE do cliente vira a arma do atacante

SAGE NETWORKS

- Nuvem de Mitigação de ataques DDoS
- Detecção de ataques DDoS
- Engenharia de redes
- SOC

e muito mais...

Motivação

- Fomos procurados por vários ISPs para investigar anomalias de tráfego análogas a DDoS, porém no sentido de UPLOAD.
- A análise aprofundada indicou que o tráfego era originado na rede de acesso dos ISPs. Mais especificamente em clientes banda larga utilizando CPEs de vendors e modelos específicos.
- Discussões e trocas de informações em grupos, fóruns e outros canais de contato da comunidade técnica ajudaram a identificar o vínculo do problema à vulnerabilidade descrita na CVE-2022-27255.

Contexto da vulnerabilidade

- **CVE-2022-27255:** vulnerabilidade de buffer overflow no **Realtek Jungle SDK**
- Afeta **roteadores, CPEs** e outros dispositivos baseados na linha de chip RTL819x
- Explorável tanto de forma local quanto remota, via pacotes UDP especialmente formatados.

Como a vulnerabilidade acontece

- Uma função de SIP ALG no SDK da Realtek, utilizada para reescrever pacotes SDP, possibilita que um pacote especialmente formatado cause um Buffer Overflow, permitindo a execução remota de código sem qualquer tipo de autenticação.
- Atacante pode utilizar esse mecanismo para **obter controle total do dispositivo** e utiliza-lo como:
  - Zumbi em botnet (Mirai, variantes)
  - Plataforma para ataques DDoS
  - Ponto de interceptação de tráfego (Man-in-the-middle)

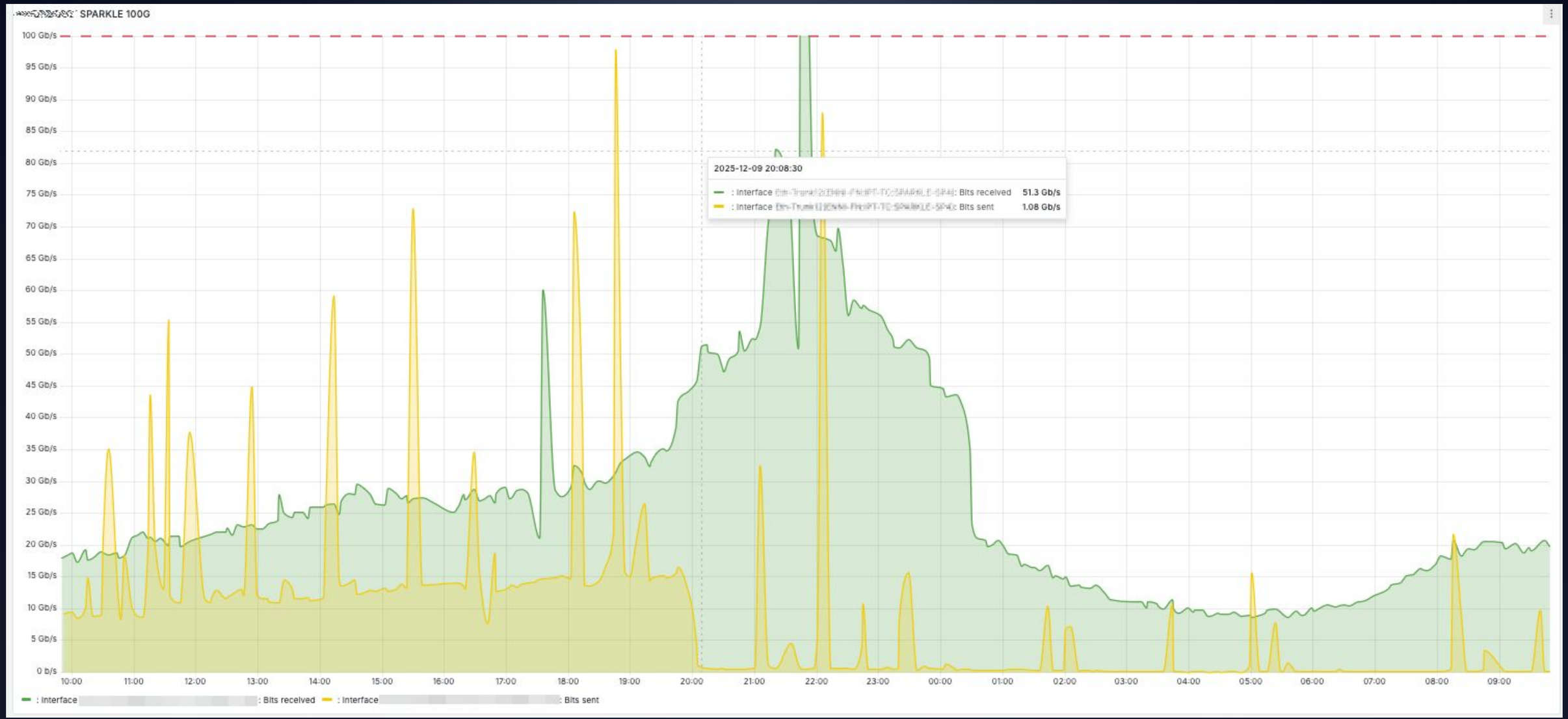
Medidas de prevenção padrão

- Modificar o usuário e senha padrão
- Controle de acesso à gerência por firewall/ACL
- Bloqueio e/ou desativação de portas e serviços desnecessários
- Políticas de atualização contínua e gestão de ciclo de vida de CPEs.
- Monitoramento proativo da rede.

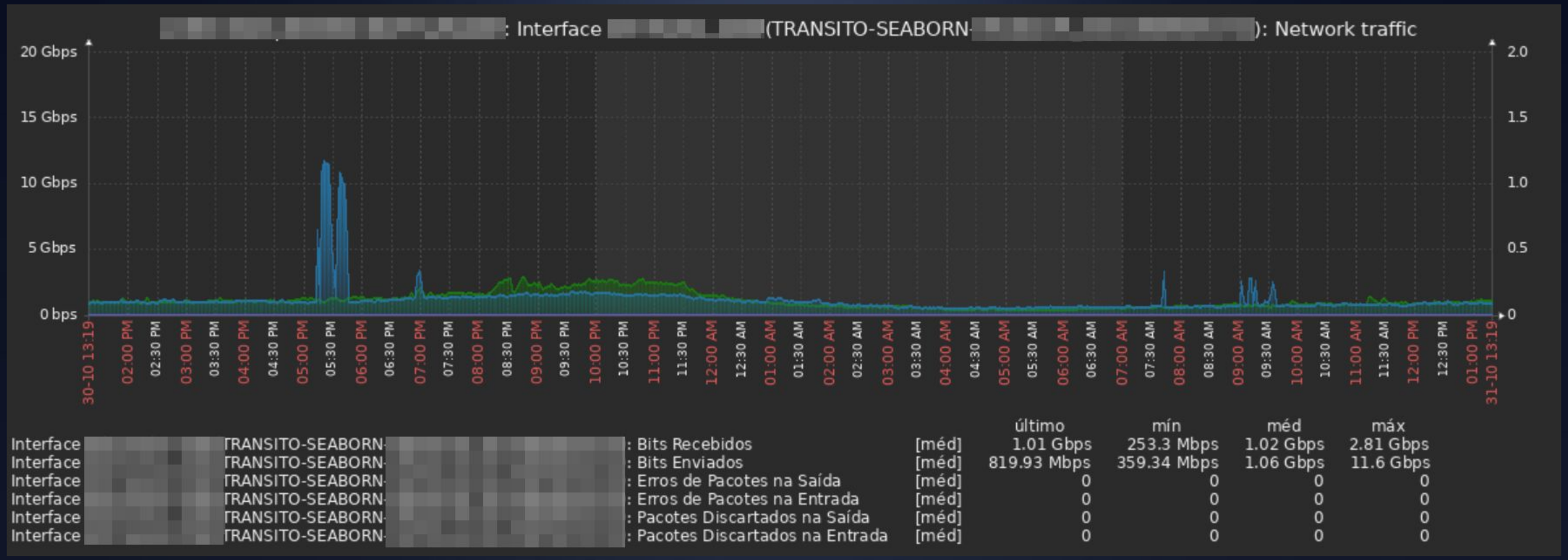
Como é percebida na rede

- Aumento anômalo de tráfego UPnP/UDP, principalmente no sentido de UPLOAD.
- Picos de CPU em CPEs comprometidos,
- Aumento no uso de recursos computacionais nos BNGs, caixas de CGNAT, etc...
- Reclamações de clientes sobre lentidão e instabilidade.

Anomalias detectadas em interface de UPSTREAM



Anomalias detectadas em interface de UPSTREAM



			último	mín	méd	máx
Interface	TRANSITO-SEABORN	: Bits Recebidos	[méd]	1.01 Gbps	253.3 Mbps	1.02 Gbps	2.81 Gbps
Interface	TRANSITO-SEABORN	: Bits Enviados	[méd]	819.93 Mbps	359.34 Mbps	1.06 Gbps	11.6 Gbps
Interface	TRANSITO-SEABORN	: Erros de Pacotes na Saída	[méd]	0	0	0	0
Interface	TRANSITO-SEABORN	: Erros de Pacotes na Entrada	[méd]	0	0	0	0
Interface	TRANSITO-SEABORN	: Pacotes Discartados na Saída	[méd]	0	0	0	0
Interface	TRANSITO-SEABORN	: Pacotes Discartados na Entrada	[méd]	0	0	0	0

Picos de uso de CPU em caixa de CGNAT

Fluxo de pacotes capturado de CPE afetada

Received Time	Start Time	Stop Time	Duration	Protocol	Src IP Address	Src Port	Src AS	Input If	Dst IP Address	Dst Port	Dst AS	Output If	TCP Flags	ToS	Packets	Bits	Pkts/s	Bits/s	Bytes/Pkt
2025-12-10 16:50:01	2025-12-10 16:49:55	2025-12-10 16:49:55	0.000	UDP	100.64.145.44	4265	0	52	168.227.62.127	26961	264876	41	.....	0	1024	11190272	0	0	1366
2025-12-10 16:50:05	2025-12-10 16:50:00	2025-12-10 16:50:00	0.000	UDP	100.64.145.44	4265	0	52	161.22.59.229	11183	262481	41	.....	0	1024	11190272	0	0	1366
2025-12-10 16:50:07	2025-12-10 16:49:59	2025-12-10 16:50:00	1.000	UDP	100.64.145.44	4265	0	52	177.11.41.219	28023	262278	41	.....	0	2048	11796480	2048	11796480	720
2025-12-10 16:50:07	2025-12-10 16:50:02	2025-12-10 16:50:02	0.000	UDP	100.64.145.44	4265	0	52	143.0.57.184	30776	52613	41	.....	0	1024	770048	0	0	94
2025-12-10 16:50:09	2025-12-10 16:50:03	2025-12-10 16:50:03	0.000	UDP	100.64.145.44	4265	0	52	170.238.250.11	35898	263959	41	.....	0	1024	11190272	0	0	1366
2025-12-10 16:50:14	2025-12-10 16:50:09	2025-12-10 16:50:09	0.000	UDP	100.64.145.44	4265	0	52	189.36.255.204	31762	270796	41	.....	0	1024	606208	0	0	74
2025-12-10 16:50:14	2025-12-10 16:50:09	2025-12-10 16:50:09	0.000	UDP	100.64.145.44	4265	0	52	170.238.250.11	35898	263959	41	.....	0	1024	11190272	0	0	1366
2025-12-10 16:50:16	2025-12-10 16:50:09	2025-12-10 16:50:09	0.000	UDP	100.64.145.44	4265	0	52	170.244.254.241	11347	28649	41	.....	0	1024	11190272	0	0	1366
2025-12-10 16:50:23	2025-12-10 16:50:16	2025-12-10 16:50:16	0.000	UDP	100.64.145.44	4265	0	52	177.11.41.219	28023	262278	41	.....	0	1024	9166848	0	0	1119
2025-12-10 16:50:23	2025-12-10 16:50:16	2025-12-10 16:50:16	0.000	UDP	100.64.145.44	4265	0	52	187.33.250.180	5552	53087	41	.....	0	1024	11190272	0	0	1366
2025-12-10 16:50:26	2025-12-10 16:50:21	2025-12-10 16:50:21	0.000	UDP	100.64.145.44	4265	0	52	189.36.255.204	31762	270796	41	.....	0	1024	606208	0	0	74
2025-12-10 16:50:26	2025-12-10 16:50:21	2025-12-10 16:50:21	0.000	UDP	100.64.145.44	4265	0	52	143.0.57.184	30776	52613	41	.....	0	1024	606208	0	0	74
2025-12-10 16:50:28	2025-12-10 16:50:22	2025-12-10 16:50:22	0.000	UDP	100.64.145.44	49339	0	52	207.174.105.89	9998	835	41	.....	0	1024	557056	0	0	68
2025-12-10 16:50:30	2025-12-10 16:50:20	2025-12-10 16:50:24	4.000	UDP	100.64.145.44	4265	0	52	168.227.62.127	26961	264876	41	.....	0	2048	22380544	512	5595136	1366
2025-12-10 16:50:30	2025-12-10 16:50:24	2025-12-10 16:50:24	0.000	UDP	100.64.145.44	4265	0	52	187.33.250.180	5552	53087	41	.....	0	2048	22380544	0	0	1366
2025-12-10 16:50:34	2025-12-10 16:50:28	2025-12-10 16:50:28	0.000	UDP	100.64.145.44	4265	0	52	143.0.57.184	30776	52613	41	.....	0	1024	606208	0	0	74
2025-12-10 16:50:37	2025-12-10 16:50:31	2025-12-10 16:50:31	0.000	UDP	100.64.145.44	4265	0	52	189.36.225.250	36789	28649	41	.....	0	1024	1048576	0	0	128
2025-12-10 16:50:38	2025-12-10 16:50:33	2025-12-10 16:50:33	0.000	UDP	100.64.145.44	4265	0	52	177.11.41.219	28023	262278	41	.....	0	1024	11190272	0	0	1366
2025-12-10 16:50:40	2025-12-10 16:50:34	2025-12-10 16:50:34	0.000	UDP	100.64.145.44	4265	0	52	186.225.74.95	39770	53172	41	.....	0	1024	606208	0	0	74
2025-12-10 16:50:45	2025-12-10 16:50:40	2025-12-10 16:50:40	0.000	UDP	100.64.145.44	4265	0	52	187.33.250.180	5552	53087	41	.....	0	1024	11190272	0	0	1366
2025-12-10 16:50:46	2025-12-10 16:50:41	2025-12-10 16:50:41	0.000	UDP	100.64.145.44	4265	0	52	143.0.57.184	30776	52613	41	.....	0	1024	606208	0	0	74
2025-12-10 16:50:47	2025-12-10 16:50:42	2025-12-10 16:50:42	0.000	UDP	100.64.145.44	4265	0	52	170.244.254.241	11347	28649	41	.....	0	1024	11190272	0	0	1366
2025-12-10 16:50:50	2025-12-10 16:50:42	2025-12-10 16:50:42	0.000	UDP	100.64.145.44	4265	0	52	189.36.255.204	31762	270796	41	.....	0	1024	606208	0	0	74
2025-12-10 16:50:53	2025-12-10 16:50:36	2025-12-10 16:50:46	10.000	UDP	100.64.145.44	24111	0	52	156.240.108.90	5178	140227	41	.....	0	83968	971341824	8396	97134182	1446
2025-12-10 16:50:57	2025-12-10 16:50:51	2025-12-10 16:50:51	0.000	UDP	100.64.145.44	4265	0	52	161.22.59.229	11183	262481	41	.....	0	1024	11190272	0	0	1366
2025-12-10 16:50:59	2025-12-10 16:50:54	2025-12-10 16:50:54	0.000	UDP	100.64.145.44	4265	0	52	186.225.74.95	39770	53172	41	.....	0	1024	770048	0	0	94
2025-12-10 16:51:07	2025-12-10 16:51:01	2025-12-10 16:51:01	0.000	UDP	100.64.145.44	4265	0	52	187.33.250.180	5552	53087	41	.....	0	1024	11190272	0	0	1366
2025-12-10 16:51:09	2025-12-10 16:50:55	2025-12-10 16:51:02	7.000	UDP	100.64.145.44	4265	0	52	143.0.57.184	30776	52613	41	.....	0	3072	1818624	438	259803	74
2025-12-10 16:51:11	2025-12-10 16:51:06	2025-12-10 16:51:06	0.000	UDP	100.64.145.44	4265	0	52	161.22.59.229	11183	262481	41	.....	0	1024	11190272	0	0	1366

Flow Records Flow Tops

Impactos para ISPs e clientes finais

- Degradação de desempenho da rede
- Gargalos nas interfaces de enlace
- Instabilidade ou indisponibilidade para o cliente
- Oneração do time técnico, suporte e ferramentas de mitigação
- Danos à reputação do ISP.

Como detectar?

- Coleta de métricas via SNMP/telemetria para identificar anomalias na linha base de tráfego da rede.
- Monitoramento de assinaturas conhecidas em IDS/IPS (Wanguard, Snort, Suricata, Team-Cymru Nimbus, etc...).
- Monitoramento proativo de vulnerabilidades (OPEN VAS)
- Análise de logs e pacotes suspeitos (ex.: pacotes UPnP não usuais).

Como corrigir?

Atualização de firmware e/ou aplicação de patches fornecidos pelos fabricantes.

Conclusão

Vulnerabilidades como a CVE-2022-27255 são como a luz da injeção acesa no painel do carro: Se você ignorá-las as consequências podem ser catastróficas.

REFERÊNCIAS E LINKS ÚTEIS

SAGENETWORKS. CVE-2022-27255. Sage Networks, [s.l.], [s.d.]. Disponível em: <https://sagenetworks.com.br/cve-2022-27255/>. Acesso em: 03 de outubro de 2025.

SAGENETWORKS. ONT malware. Sage Networks, [s.l.], [s.d.]. Disponível em: <https://sagenetworks.com.br/ont-malware/>. Acesso em: 03 de outubro de 2025.

MITRE. CVE-2022-27255. CVE.org, [s.l.], [s.d.]. Disponível em: <https://www.cve.org/CVERecord?id=2022-27255>. Acesso em: 03 de outubro de 2025.

NIST. Detalhe da vulnerabilidade CVE-2022-27255. NVD (National Vulnerability Database), [s.l.], [s.d.]. Disponível em: <https://nvd.nist.gov/vuln/detail/cve-2022-27255>. Acesso em: 03 de outubro de 2025.

REALTEK. Realtek_APRouter_SDK_Advisory-CVE-2022-27255. Realtek, [s.l.], [s.d.]. Disponível em: <https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2022-27255.pdf>. Acesso em: 03 de outubro de 2025.

INFOBYTE. cve-2022-27255. GitHub, [s.l.], [s.d.]. Disponível em: <https://github.com/infobyte/cve-2022-27255>. Acesso em: 03 de outubro de 2025.

SAGE NETWORKS

WWW.SAGENETWORKS.COM.BR

sage_networks Sage Networks +55 (19) 3500-6269