

TLP: CLEAR



BOLETIM DE SEGURANÇA

**Vulnerabilidades em clientes nativos da AWS permitem
ataques Man-in-the-Middle**

Acesse a nossa nova comunidade através do
WhatsApp!

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



ISH

CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH

ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH

GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como ClOp está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

SUMÁRIO

1	Introdução executiva.....	4
2	Informações sobre as vulnerabilidades.....	5
2.1	Sistemas e produtos afetados	5
2.2	Impacto da vulnerabilidade	6
3	Recomendações.....	7
4	Referências	8
5	Autores.....	8

1 INTRODUÇÃO EXECUTIVA

A Amazon Web Services (AWS) [identificou](#) e corrigiu duas vulnerabilidades, **CVE-2025-0500** e **CVE-2025-0501**, que afetavam versões específicas dos clientes nativos do **Amazon WorkSpaces**, **Amazon AppStream 2.0** e **Amazon DCV**. Essas falhas poderiam permitir que agentes mal-intencionados realizassem ataques man-in-the-middle, comprometendo a segurança das sessões remotas dos usuários.

2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

A vulnerabilidade [CVE-2025-0500](#) residia nos clientes nativos dos serviços Amazon WorkSpaces, Amazon AppStream 2.0 e Amazon DCV, permitindo que atacantes interceptassem e manipulassem o tráfego entre o cliente e o servidor, potencialmente comprometendo a confidencialidade e integridade dos dados transmitidos.

A [CVE-2025-0501](#) afetava especificamente os clientes do Amazon WorkSpaces que utilizavam o protocolo PCoIP, expondo-os a riscos semelhantes de interceptação e acesso não autorizado. A exploração dessas vulnerabilidades poderia permitir que atacantes realizassem ataques man-in-the-middle, interceptando e potencialmente modificando dados transmitidos entre o cliente e o servidor. Isso colocaria em risco informações sensíveis e a integridade das sessões remotas dos usuários.

2.1 SISTEMAS E PRODUTOS AFETADOS

Abaixo segue as informações referente aos produtos e versões afetadas pelas falhas:

CVE-2025-0500

- **Amazon WorkSpaces:**
 - Cliente Windows versão 5.20.0 ou anterior
 - Cliente macOS versão 5.20.0 ou anterior
 - Cliente Linux versão 2024.1 ou anterior
- **Amazon AppStream 2.0:**
 - Cliente Windows versão 1.1.1326 ou anterior
- **Amazon DCV:**
 - Cliente Windows versão 2023.1.8993 ou anterior
 - Cliente macOS versão 2023.1.6203 ou anterior
 - Cliente Linux versão 2023.1.6203 ou anterior

CVE-2025-0501

- **Amazon WorkSpaces:**
 - Cliente Windows versão 5.22.0 ou anterior
 - Cliente macOS versão 5.22.0 ou anterior
 - Cliente Linux versão 2024.5 ou anterior
 - Cliente Android versão 5.0.0 ou anterior

2.2 IMPACTO DA VULNERABILIDADE

Caso exploradas, as vulnerabilidades podem resultar em:

- Acesso não autorizado.
- Comprometimento de dados e execução de comandos maliciosos.
- Interrupção de serviços críticos.

3 RECOMENDAÇÕES

É altamente recomendável que os usuários atualizem imediatamente seus clientes para as versões corrigidas:

Amazon WorkSpaces

- Atualizar para a versão *5.21.0* ou superior no Windows e macOS, e para a versão *2024.2* ou superior no Linux.

Amazon AppStream 2.0

- Atualizar para a versão *1.1.1332* ou superior no Windows.

Amazon DCV

- Atualizar para a versão *2023.1.9127* ou superior em todas as plataformas.

4 REFERÊNCIAS

- **Heimdall by ISH Tecnologia**
- [AWS](#)
- [CVE](#)
- [Cyber Security News](#)

5 AUTORES

- **Rafael Salomé**



heimdall
security research

A DIVISION OF ISH