



Análise Experimental de Vulnerabilidades no Dispositivo Amazon Echo Pop

Murilo Henrique Galvão De Sousa Azevedo | murilo.hgs@aluno.ifsc.edu.br¹

Maykon Chagas | maykon.chagas@ifsc.edu.br²

Andrei de Souza Inácio | andrei.inacio@ifsc.edu.br³

Edital nº 02/2025/PROPPI - PIBIC

Trabalho de Pesquisa

DT 4 - Inovação Tecnológica, Processos Produtivos e Futuro das Tecnologias

Resumo:

O crescente uso do Amazon Echo Pop em ambientes domésticos e empresariais traz preocupações quanto aos riscos à segurança e à privacidade inerentes ao uso de assistentes virtuais. Este estudo objetiva mapear as vulnerabilidades vindas de literaturas acadêmicas e testar as vulnerabilidades do dispositivo para fornecer subsídios metodológicos a futuras pesquisas e correções do fabricante. A metodologia integrou uma revisão bibliográfica de ataques e vulnerabilidades registradas, com a execução prática de explorações em ambiente controlado. Os testes práticos indicaram resiliência do dispositivo, mas ainda há vulnerabilidades que podem comprometer a privacidade e os dados sensíveis do usuário.

Palavras-chave: cibersegurança; segurança da informação; Alexa; internet das coisas.

Introdução

O uso dos dispositivos da Amazon tem crescido de maneira exponencial em escala global e nacional. No Brasil, estimativas indicam que em 2025, os usuários executaram cerca de dois bilhões de rotinas na Alexa (Amazon, 2026). A assistente virtual da Amazon, popularmente conhecida como "Alexa" desempenha um papel central na automação residencial, gerenciando desde tarefas cotidianas, como: controle de iluminação, reprodução de mídia e agendamentos, até a realização de compras dentro do aplicativo da Amazon (Amazon, 2025). Diante do expressivo uso e das diversas funcionalidades operadas por comando de voz, a segurança da informação surge como um desafio crítico. A privacidade e a proteção de dados de uma grande parte dos usuários encontra-se potencialmente vulnerável, uma vez que informações sensíveis e o monitoramento de rotinas fluem continuamente por meio desses dispositivos. Desse

¹ Estudante do curso Superior em Análise e Desenvolvimento de Sistemas do IFSC - Câmpus Gaspar.

² Professor da área de Informática do IFSC, Câmpus Florianópolis.

³ Professor da área de Informática do IFSC, Câmpus Gaspar.

modo, o presente estudo tem como objetivo principal mapear e testar, as vulnerabilidades do dispositivo Amazon Echo Pop previamente reportadas na literatura acadêmica e em relatórios técnicos.

Fundamentação teórica

A arquitetura do Echo Pop é composta por um núcleo de serviços conectado à nuvem da Alexa para o processamento de comandos de voz e linguagem natural. Sua estrutura permite expansão via aplicações de terceiros, denominadas *skills*, que ampliam suas funcionalidades (Pathak *et al.*, 2022).

Nesse contexto, a segurança desse ambiente de Internet das Coisas (IoT) pode ser analisada a partir da tríade CID (Confidencialidade, Integridade e Disponibilidade). A confidencialidade refere-se à proteção das informações contra acessos não autorizados; a integridade garante que os dados não sejam alterados indevidamente; e a disponibilidade assegura o acesso aos sistemas e informações sempre que necessário (Stallings; Brown, 2014).

Diante disso, a literatura acadêmica tem documentado vulnerabilidades vindas do dispositivo Echo Pop. Os vetores de ataque mapeados exploram desde a camada de aplicação, até vulnerabilidades estruturais nos protocolos de comunicação, como vulnerabilidades na interface Bluetooth (Esposito *et al.*, 2020) e nas *skills* do dispositivo (Pathak *et al.*, 2022). Ao reproduzir e testar essas vulnerabilidades em laboratório, a pesquisa consolida a fundamentação teórica de cibersegurança e Internet das Coisas, cumprindo um papel social ao investigar se fabricantes corrigiram as vulnerabilidades que expõem os usuários a riscos.

Procedimentos metodológicos

A presente pesquisa caracteriza-se como aplicada, de abordagem qualitativa, com caráter exploratório e descritivo, utilizando como estratégia a pesquisa bibliográfica aliada à experimentação em ambiente controlado (Prodanov; Freitas, 2013). Inicialmente, foi realizada uma revisão da literatura em bases acadêmicas e relatórios técnicos, com o objetivo de identificar vulnerabilidades associadas ao Echo Pop. Em seguida, as vulnerabilidades mais relevantes foram selecionadas com base em sua aplicabilidade e

impacto potencial. Na etapa experimental, os cenários de ataque foram reproduzidos em laboratório, permitindo observar o comportamento do dispositivo diante das tentativas de exploração. Os testes foram documentados e, posteriormente, as vulnerabilidades foram classificadas com base no padrão CVSS (Common Vulnerability Scoring System), que fornece um método padronizado para capturar as principais características de uma vulnerabilidade e calcular uma pontuação numérica de severidade, que pode ser convertida em níveis qualitativos (baixo, médio, alto) para apoiar a priorização no gerenciamento de vulnerabilidades.

Resultados e discussões

Os resultados obtidos estão sintetizados no Quadro 1, as vulnerabilidades do Echo Pop reportadas na literatura (1 a 5), além das vulnerabilidades identificadas durante a etapa experimental (6 a 8). Estas vulnerabilidades concentram-se na camada de aplicação, abrangendo a execução de comandos indevidos e o uso de *skills* maliciosas. De maneira geral, o dispositivo demonstrou nível satisfatório de segurança, especialmente contra ataques diretos.

No entanto, foram observadas fragilidades nos protocolos de comunicação, como no pareamento Bluetooth e na troca de dados, o que pode ampliar o vetor de ataque. Embora muitas vulnerabilidades apresentem risco baixo a médio segundo o CVSS, sua exploração combinada pode comprometer a confidencialidade das informações. É importante ressaltar que as vulnerabilidades identificadas nas *skills* foram exploradas em ambiente local e controlado, não havendo submissão ou validação junto aos mecanismos de revisão da Amazon. Ainda assim, a possibilidade de exploração, mesmo restrita a esse contexto, torna possível o comprometimento da confidencialidade das informações em casos reais. Além disso, destaca-se a presença de vetores de engenharia social, evidenciando o papel do usuário na segurança do sistema. Assim, conclui-se que o dispositivo apresenta segurança adequada ao seu contexto de uso, mas ainda requer melhorias, especialmente na proteção da privacidade e no controle de acesso.

Quadro 1 - Caracterização e classificação das vulnerabilidades encontradas

ID	Vulnerabilidade	Descrição	Impacto	Nível de Risco
1	Alexa VS Alexa	O dispositivo é capaz de captar e processar comandos de voz emitidos pelos seus próprios alto-falantes, desde que o volume esteja no máximo e haja pausas estratégicas no áudio.	Se um atacante reproduzir um áudio malicioso pelo dispositivo, pode induzir a Alexa a executar ações sensíveis sem autenticação do usuário legítimo.	1.9 / Low
2	Voice Squatting	Possibilidade de criar e invocar <i>skills</i> utilizando nomes de invocação foneticamente idênticos ou confusos em relação a serviços legítimos (ex: "ge hum" para imitar "G1").	Um usuário pode acionar acidentalmente a <i>skill</i> maliciosa do atacante achando que é a oficial, permitindo o roubo de dados, senhas faladas ou execução de rotinas não autorizadas.	1.6 / Low
3	Ausência de Autenticação Forte no Pareamento Bluetooth	O dispositivo permite o pareamento Bluetooth apenas com o comando de voz, sem exigir confirmação de duplo fator ou aprovação dentro do aplicativo Alexa.	Um invasor com acesso físico pode emparelhar um dispositivo e usá-lo de forma maliciosa.	5.6 / Medium
4	Mask Attack	A vulnerabilidade ocorre quando o atacante intercepta uma <i>utterance</i> específica do usuário na <i>skill</i> e a encaminha a um oráculo externo, que gera uma resposta válida e a retorna, permitindo a manipulação do comportamento da aplicação.	O atacante pode capturar informações sensíveis do usuário, além de conseguir deixar a Alexa inativa por mais de 10s, sem receber nenhum comando, tornando ela inútil.	4.2 / Medium
5	Bypass da API de informações	A vulnerabilidade permite a coleta de	O atacante pode guardar as informações ditas pelo	7 / High

	sensíveis	dados sensíveis (como número de telefone) sem uso de API oficial. A <i>skill</i> pode capturar essas informações e armazená-las no banco de dados disponibilizado pela Amazon.	cliente para usar posteriormente para alguma finalidade. Podendo direcionar golpes para aquela pessoa em questão.	
6	Vazamento de Metadados e Padrão de Comportamento	Mesmo não conseguindo quebrar a criptografia TLS para ler os pacotes em claro durante a tentativa de MitM, os metadados vazados são suficientes para identificar o hardware.	Risco à segurança física e privacidade. Um atacante na mesma rede pode analisar o gráfico de tráfego para deduzir exatamente os horários em que a casa está ocupada e ativa.	6.1 / Medium
7	Negação de Serviço (DoS) Local via ARP Spoofing	O dispositivo não possui defesas nativas robustas contra envenenamento de tabela ARP na rede local.	Indisponibilidade do dispositivo (DoS). O usuário perde o controle da automação residencial e do assistente.	6 / Medium
8	Interceptação e Vazamento de Áudio	Uma vez pareado, o computador do atacante é reconhecido como saída de áudio de confiança. Todas as respostas da Alexa são transmitidas para a máquina do atacante.	Comprometimento de privacidade: o atacante pode capturar e registrar as respostas da Alexa.	6.8 / Medium

Fonte: elaborada pelo autor a partir de análises realizadas na métrica do CVSS.

Considerações finais

Os objetivos propostos neste trabalho foram alcançados, todos os testes planejados foram executados, identificando vulnerabilidades no dispositivo. A combinação de procedimentos metodológicos, envolvendo revisão bibliográfica e experimentação em ambiente controlado, mostrou-se adequada para a validação prática das vulnerabilidades.



A atividade contribuiu para a formação acadêmica e profissional ao viabilizar a aplicação prática dos conhecimentos. A principal limitação foi o tempo reduzido para testes, restringindo a exploração de alguns cenários. Ainda assim, os resultados representam avanço na identificação de vulnerabilidades e na análise do comportamento do dispositivo sob ataque. Além disso, o estudo apresenta potencial para pesquisas futuras, servindo como base para investigações mais aprofundadas sobre a segurança do Echo Pop.

Referência ao fomento recebido

Os autores agradecem o Instituto Federal de Santa Catarina - IFSC, que por meio do Edital Nº 02/2025/PROPI/PIBIC, possibilitou a realização do projeto.

Referências

AMAZON. **Alexa em 2025**: a assistente de voz cada vez mais presente no dia a dia dos brasileiros. [S. l.], 2026. Disponível em: <https://www.aboutamazon.com.br/noticias/dispositivos/alexa-em-2025-a-assistente-de-voz-cada-vez-mais-presente-no-dia-a-dia-dos-brasileiros>. Acesso em: 16 abr. 2026.

AMAZON. **Alexa for Apps**. [S. l.], 2025. Disponível em: <https://developer.amazon.com/en-US/docs/alexa/alexa-for-apps/about-alexa-for-apps.html>. Acesso em: 16 abr. 2026.

ESPOSITO, Sergio; SGANDURRA, Daniele; BELLA, Giampaolo; O'KEEFFE, Daniel. The Alexa versus Alexa attack: hacking voice-controllable devices. In: ACM ASIA CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY (ASIA CCS), 15., 2020, New York. **Proceedings** [...] New York: ACM, 2020.

FIRST. **Common Vulnerability Scoring System (CVSS)**. Forum of Incident Response and Security Teams, 2026. Disponível em: <https://www.first.org/cvss/>. Acesso em: 16 abr. 2026.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Feevale, 2013.



PATHAK, Surendra; ISLAM, Sheikh Ariful; JIANG, Honglu; XU, Lei; TOMAI, Emmett. A survey on security analysis of Amazon echo devices. **High-Confidence Computing**, [S.l.], v. 2, n. 4, p. 100087, dez. 2022. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2667295222000393>. Acesso em: 16 abr. 2026.

STALLINGS, William; BROWN, Lawrie. **Segurança de computadores: princípios e práticas**. 2. ed. São Paulo: Pearson Education do Brasil, 2014.