BOLETIM DE SEGURANÇA

Falhas críticas RCE do ServiceNow sendo exploradas em ataques

heimdall
security research
A DIVISION OF ISH

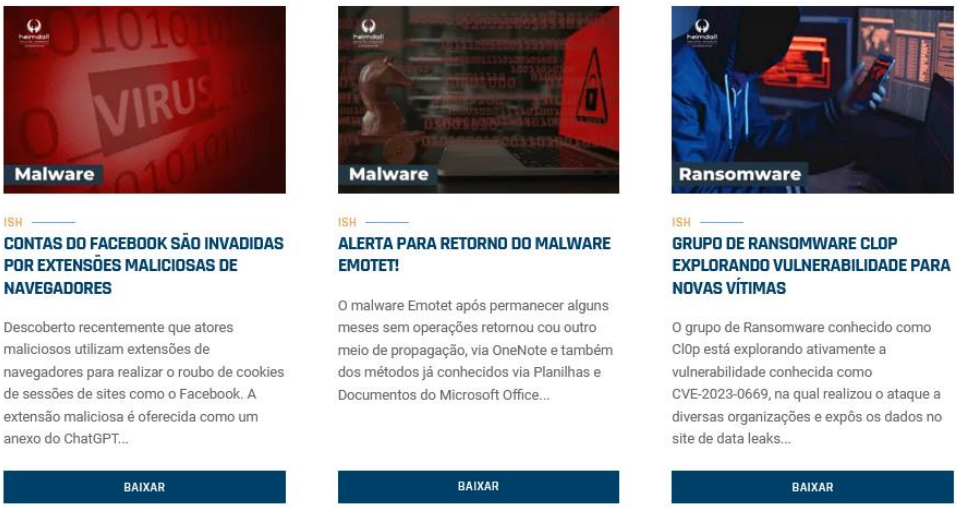
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[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]



SUMÁRIO

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Foi observado recentemente que atores de ameaças estão encadeando as falhas **CVE-2024-4879**, **CVE-2024-5217** e **CVE-2024-5178** do ***ServiceNow*** e usando exploits públicos para violar agências governamentais e organizações privadas em ataques de roubo de dados.

2 DETALHES SOBRE AS VULNERABILIDADES

CVE-2024-4879

Esta vulnerabilidade de injeção de template Jelly permite que usuários não autenticados executem código arbitrário dentro do contexto da plataforma Now. Foi identificada nas versões Vancouver e Washington DC do ServiceNow.

- **Impacto**: Possibilita a execução remota de código, comprometendo a confidencialidade, integridade e disponibilidade do sistema afetado.
- **Pontuação CVSS**: 9.3 (Crítica).

CVE-2024-5217

Esta vulnerabilidade de validação de entrada também permite a execução remota de código por um usuário não autenticado. Foi identificada nas versões Washington DC, Vancouver e anteriores da plataforma Now.

- **Impacto**: Semelhante à CVE-2024-4879, possibilita que atacantes executem código arbitrário, resultando em potencial comprometimento completo do sistema, roubo de dados e interrupção de operações críticas.
- **Pontuação CVSS**: 9.8 (Crítica).

CVE-2024-5178

Esta vulnerabilidade permite que usuários administrativos obtenham acesso não autorizado a arquivos sensíveis no servidor da aplicação web.

- **Impacto**: Embora menos severa que as outras duas, ainda apresenta um risco significativo de exposição de dados e acesso não autorizado a informações confidenciais.
- **Pontuação CVSS**: 6.5 (Média).

Versões do ServiceNow afetadas pelas vulnerabilidade:

- *Afetado de 0 antes do Utah Patch 10 Hot Fix 3*
- *Afetado de 0 antes do Utah Patch 10a Hot Fix 2*
- *Afetado de 0 antes do Vancouver Patch 6 Hot Fix 2*
- *Afetado de 0 antes do Vancouver Patch 7 Hot Fix 3b*
- *Afetado de 0 antes do Vancouver Patch 8 Hot Fix 4*
- *Afetado de 0 antes do Vancouver Patch 9 Hot Fix 1*
- *Afetado de 0 antes do Vancouver Patch 9*
- *Afetado de 0 antes do Vancouver Patch 10*
- *Afetado de 0 antes do Washington DC Patch 1 Hot Fix 2b*
- *Afetado de 0 antes do Washington DC Patch 1 Hot Fix 3b*
- *Afetado de 0 antes do Washington DC Patch 2 Hot Fix 2*
- *Afetado de 0 antes do Washington DC Patch 3 Hot Fix 1*
- *Afetado de 0 antes do Washington DC Patch 4*

- *Afetado de 0 antes do Washington DC Patch 5*

3 LARGA UTILIZAÇÃO DA PLATAFORMA E EXPLORAÇÕES DAS FALHAS

Com auxilio de ferramentas de Inteligência foi possível observar milhares de instâncias do ServiceNow expostas pela Internet em vários países ao redor do mundo, o que agrava a situação das falhas.

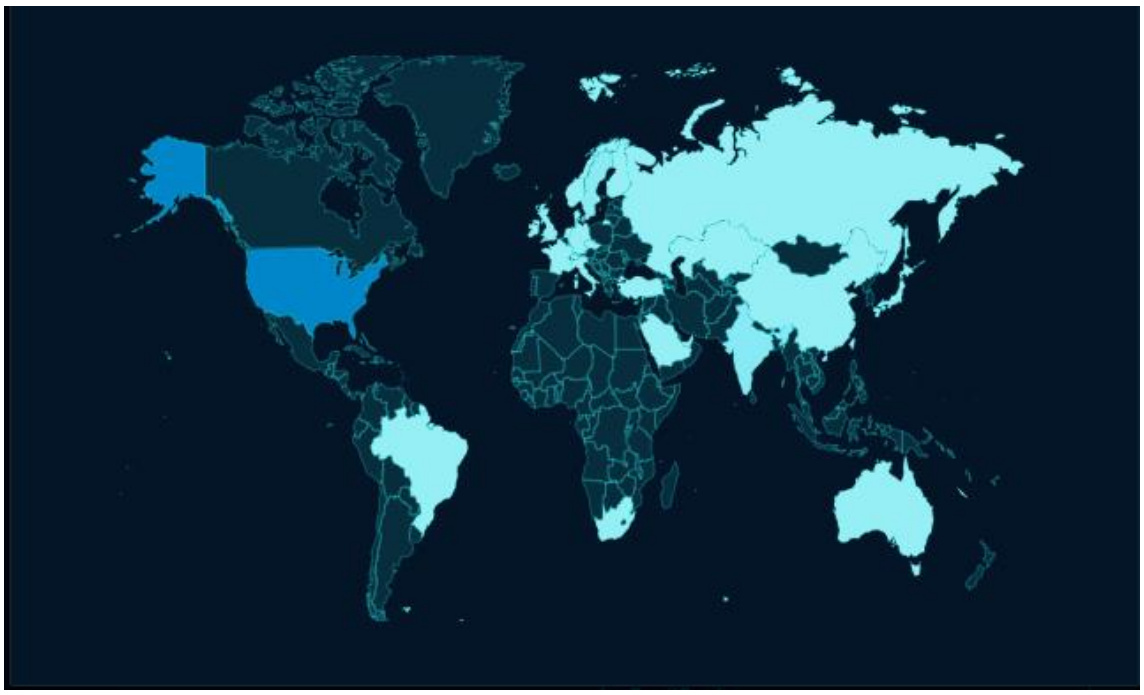


Figura 1 – Instancias do ServiceNow expostas na Internet.

Devido as publicações de exploits públicos com base nas falhas, pesquisadores de segurança já observaram varreduras para explorações em massa das falhas, o que requer uma grande atenção por parte dos administradores que utilizam a plataforma para uma rápida atualização com os *Patches e Hotifixes* disponibilizados pela ServiceNow.

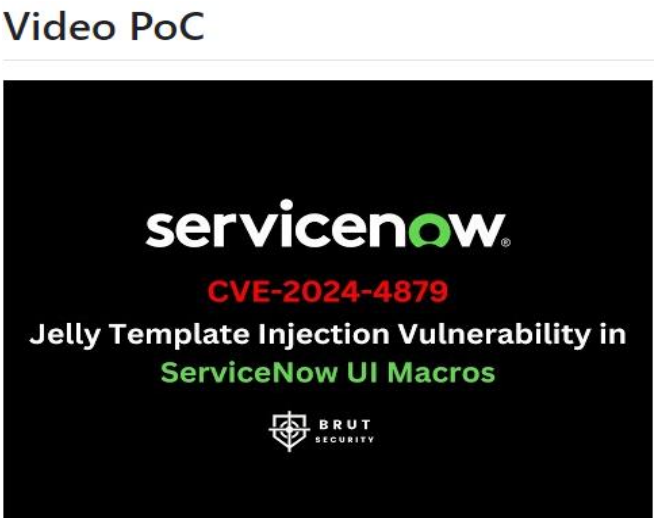


Figura 2 – Print de um vídeo de PoC disponibilizada no GitHub.

4 CONCLUSÃO

A exploração de vulnerabilidades no ServiceNow pode causar graves danos às organizações. Esses riscos incluem a perda de dados sensíveis, como informações de clientes e registros financeiros, comprometendo a privacidade e a segurança da informação. Além disso, a interrupção dos serviços críticos pode ocorrer, afetando a continuidade dos negócios e a eficiência operacional. A exploração de falhas pode permitir que agentes maliciosos manipulem ou destruam dados, resultando em custos elevados para recuperação e restauração. Além disso, a reputação da organização pode ser severamente prejudicada, impactando a confiança dos clientes e parceiros. As penalidades legais também são uma preocupação, devido à falha em proteger adequadamente os dados e sistemas.

5 RECOMENDAÇÕES

São elencadas abaixo pela ISH, medidas que poderão ser adotadas visando a mitigação da referida *ameaça*, como por exemplo:

- Aplique imediatamente os patches e hotfixes fornecidos pela ServiceNow para corrigir essas vulnerabilidades. A ServiceNow lançou atualizações específicas em junho de 2024 para resolver essas falhas.
- Revisão de configurações de segurança, verifique e ajuste as configurações de segurança do ServiceNow para garantir que estejam alinhadas com as melhores práticas de segurança. Isso inclui revisar políticas de acesso, permissões de usuário e configurações de firewall.
- Monitoramento contínuo, implemente ferramentas de monitoramento para detectar atividades suspeitas ou tentativas de exploração. Isso pode ajudar a identificar rapidamente qualquer tentativa de ataque e responder de maneira eficaz.
- Treinamento e conscientização, eduque os usuários e administradores sobre as vulnerabilidades e as melhores práticas de segurança. Isso pode incluir treinamentos regulares e atualizações sobre novas ameaças e vulnerabilidades.
- Revisão de logs e auditorias, regularmente revisar logs de sistema e realizar auditorias de segurança para detectar quaisquer anomalias ou atividades não autorizadas.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Support.servicenow
- NVD
- Resecurity
- Bleepingcomputer

7 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH