heimdall

security research

A DIVISION OF ISH

Nova falha de segurança crítica descoberta no software PaperCut

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

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

1 Software Papercut 6
2 Nova falha de segurança no software 7
3 Servidores Papercut Visualizados 8
4 Detecção 10
5 Conclusão 11
6 Recomendações 12
7 Referências 13

Lista de Figuras

Figura 1 – Servidores Papercut no Mundo. 8
Figura 2 – Servidores Papercut no Brasil. 8
Figura 3 – Mapa por cidades brasileiras. 9

1 SOFTWARE PAPERCUT

O PaperCut é um software de gerenciamento de impressão e cópia que ajuda as empresas a monitorar e controlar seus custos de impressão, além de aumentar a segurança da impressão e promover práticas mais sustentáveis. Com o PaperCut, os usuários podem gerenciar impressoras de vários fornecedores em uma única interface, definir quotas de impressão e copia por usuário, departamento ou cliente, restringir o acesso a determinadas funções de impressão e criar relatórios detalhados sobre o uso da impressão.

O software é usado em diversos tipos de organizações, desde pequenas empresas até grandes universidades e empresas multinacionais, e está disponível em diferentes versões para atender às necessidades específicas de cada empresa.

2 NOVA FALHA DE SEGURANÇA NO SOFTWARE

Recentemente foi descoberta por pesquisadores, uma nova falha de segurança classificada como crítica no software PaperCut NG e PaperCut MF afetando as versões anteriores a **22.1.3** no **Windows**, a qual permite execução remota de código (*RCE*), onde invasores podem carregar, ler ou excluir arquivos arbitrários.

CVE-2023-39143 - PaperCut NG/MF

Pontuação: 9.8 – Critica

Vetor: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

3 SERVIDORES PAPERCUT VISUALIZADOS

Segue abaixo imagem da pesquisa por servidores papercut ao redor do mundo.

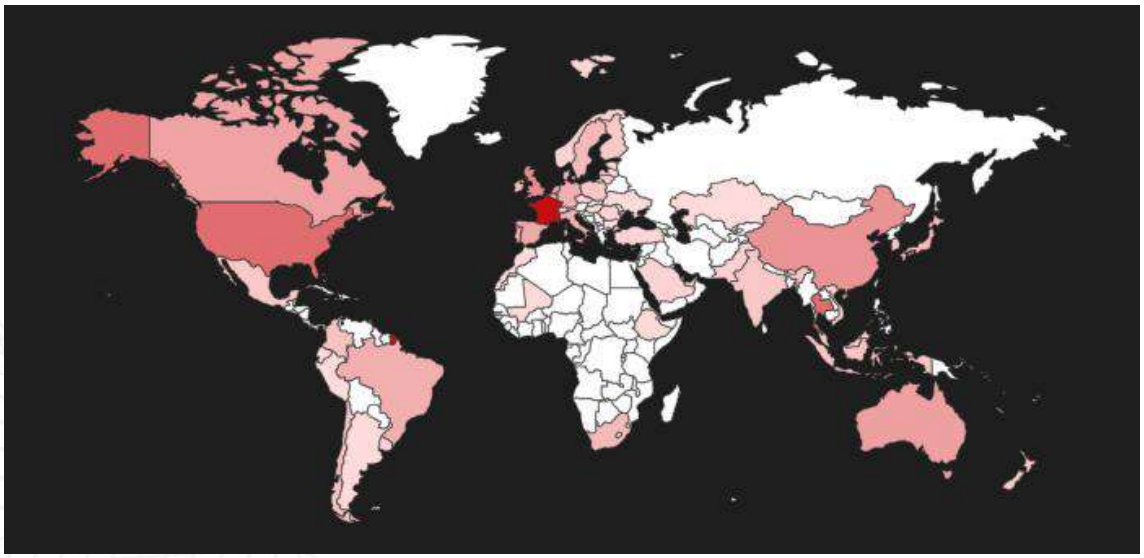

Figura 1 – Servidores Papercut no Mundo.

Em buscas realizadas através do Shodan foram encontrados "cerca" de **29 servidores** papercut associados ao **Brasil**, isso com base na consulta para encontrar Papercut no HTML pois a porta padrão é 9191, mas pode ser mudada e sendo possível a existência de mais servidores no país.

Figura 2 – Servidores Papercut no Brasil.

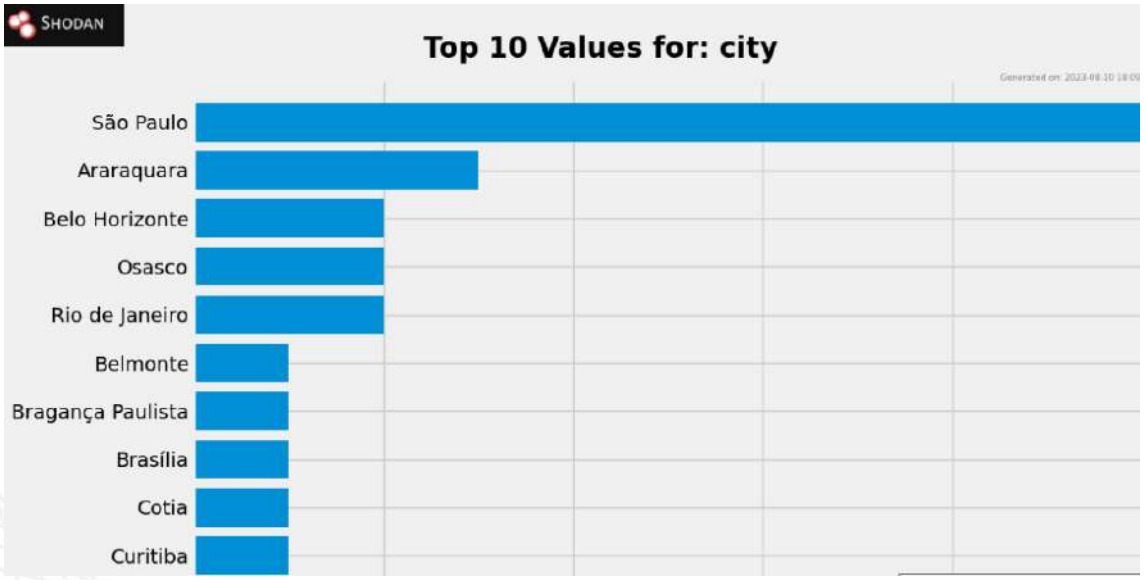

Figura 3 – Mapa por cidades brasileiras.

4 DETECÇÃO

Para detecção desta vulnerabilidade pode ser usado o comando abaixo, o mesmo verifica se o servidor está corrigido e se está sendo executado no Windows.

curl -w "%{http_code}" -k --path-as-is "https://<IP>:<port>/custom-report-example/..\..\..\deployment\sharp\ icons\home-app.png"

5 Conclusão

Devido ao alto risco de exploração e criticidade da vulnerabilidade mencionada neste boletim de ameaças, destacamos a importância de abordar vulnerabilidades de maneira proativa e eficaz.

A exploração de vulnerabilidades em produtos demonstra as sérias ramificações que podem resultar da negligência na segurança cibernética. Casos notórios, como ataques de ransomware, vazamentos massivos de dados e comprometimento de sistemas críticos, ressaltam a necessidade de empresas e desenvolvedores priorizarem a identificação, mitigação e correção contínua de vulnerabilidades.

6 RECOMENDAÇÕES

Além do método de detecção indicado pela ISH, poderão ser adotadas medidas visando a mitigação da referida *vulnerabilidade*, como por exemplo:

- **Atualização do servidor Papercut** para uma versão corrigida, segue a manual de procedimento da atualização repassado pela própria Papercut.
- **Adoção e medidas de proteção de borda,** como *Firewall*, IDS/IPS, *Honeypots*, MDR/XDR e outras soluções de segurança.
- **Adoção de medidas de antivírus,** visando verificar e varrer constantemente toda a infraestrutura e ativos utilizados.

7 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Papercut**
- **Horizon**
- **NVD**
- **Shodan.io**

heimdall
security research

A DIVISION OF ISH