Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

huntresslabs / threat-intel Public

Notifications Fork 5 Star 28

Code Issues Pull requests 2 Actions Projects Security Insights

Files

main

Go to file

- 2022
- 2023
  - 2023-02
  - 2023-03
  - 2023-04/20-PaperCut
    - win_susp_papercut_code_exec...
  - 2023-06
  - 2023-11
- 2024
- .gitignore
- LICENSE
- README.md

threat-intel / 2023 / 2023-04 / 20-PaperCut / win_susp_papercut_code_execution.yml

gleeda renaming directory aaca2c8 · last year History

Code Blame 16 lines (16 loc) · 429 Bytes Raw

```yaml
title: PaperCut MF/NG Vulnerability
authors: Huntress DE&TH Team
description: Detects suspicious code execution from vulnerable PaperCut versions MF and
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    ParentImage|endswith: "\\pc-app.exe"
    Image|endswith:
      - "\\cmd.exe"
      - "\\powershell.exe"
  condition: selection
level: high
falsepositives:
    - Expected admin activity
```