Sign in

huntresslabs / **threat-intel** Public

Notifications Fork 5 Star 28

Code Issues Pull requests 1 Actions Projects Security Insights

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

16 lines (16 loc) · 429 Bytes

Code Blame Raw

```yaml
title: PaperCut MF/NG Vulnerability
authors: Huntress DE&TH Team
description: Detects suspicious code execution from vulnerable PaperCut versions MF and NG
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
```