```
############ README ###############
##  - This is not a conventional Sigma rule. Please do not edit "logsource-product: blank" unless you are editing this rule to meet specific logsources/fields and know your environment.
##  - Query may a take long time to process.
##  - Ensure your EDR/SIEM instance has enough memory to run these AND/OR condition based queries.
##  - Analyst may need to make adjustments to the query as required. Sometimes simpler does it. However, these rules provide full list of IOCs.
##  - TLP GREEN + Please use local installation of Sigma to convert this rule.
##  - TLP CLEAR may convert rules using (https://uncoder.io/ or https://sigconverter.io/)
##CISA Code & Media Analysis
###################################

title: Detects RESURGE Malware Activity Ivanti CVE 2025_0282
tlp: CLEAR
id: d26745fc-7a56-4ca9-9011-7ab416d14875
status: test
description: Detects RESURGE Malware Activity Ivanti CVE 2025_0282 as described in MAR-25993211.r1.v1. Some strings may have high FP. Analyst must adjust as needed.
references:
    - 25993211.r1.v1
    - 52bbc44eb451cb5e16bf98bc5b1823d2f47a18d71f14543b460395a1c1b1aeda
author: CISA Code & Media Analysis
date: 2025-03-28
modified: 2025-03-28
logsource:
    product: blank
detection:
    keywords:
        - '/bin/mkdir /tmp/new_img'
        - '/bin/dsmain -g'
        - '/tmp/installer/do-install-coreboot'

    keywords_1:
        - 'sed -i'

    keywords_2:
        - '"1i/lib/%s"'
        - 'ld.so.preload'
        - 'Extracting Package'
        - 'Saving package'
        - 'clean'
        - 'LD_PRELOAD'
        - 'DSUpgrade.pm'
        - 'check_integrity.sh'
        - 'coreboot.img'
        - 'boot'
        - 'compcheckresult.cgi'
```

```
    - '/tmp/data/root/home/etc/manifest/manifest'
    - 'manifest'

keywords_3:
    - 'cp'

keywords_4:
    - '/lib/%s /tmp/data/root/lib'
    - '/lib/%s'
    - '/tmp/data/root/lib'
    - 'scanner*.egg'
    - '/bin/dsmain /tmp/coreboot_fs/bin/dsmain'
    - '/tmp/coreboot_fs'
    - '/home/root/lib/%s'
    - 'dsmain'

keywords_5:
    - 'openssl'

keywords_6:
    - 'dgst -sha256'
    - 'genrsa -out'
    - 'rsa -in'
    - 'dgst -sha512'

keywords_7:
    - '/tmp/data/root/home/perl/DSUpgrade.pm'
    - '/tmp/data/root/home/webserver/htdocs/'
    - 'check_integrity.sh'
    - 'private.pem'
    - 'manifest'

keywords_8:
    - 'system'
    - 'sed -i'

keywords_9:
    - 'mismatch*'
    - 'newFiles*'

keywords_10:
    - 'pass'
    - 'scanner*.py'

keywords_11:
    - '/bin/dsmain'

keywords_12:
    - 'gunzip'
    - 'gzip'
```

```
    - 'cpio'
    - '-idvm'
    - 'touch'
    - 'sed -i'
    - 'find'
    - 'strings'
    - '-e'
    - '-d'
    - '-s'

keywords_13:
    - 'coreboot.img*'
    - 'coreboot_fs'
    - 'ld.so.preload'
    - 'vmlinux'
    - 'version'

keywords_14:
    - '/bin/rm'
    - 'rm'

keywords_15:
    - '*vmlinux.sh'
    - 'coreboot.img.1'
    - 'coreboot_fs'
    - 'private.pem'

keywords_16:
    - 'mv'

keywords_17:
    - 'manifest*'

keywords_18:
    - 'touch'
keywords_19:
    - 'ld.so.preload'

keywords_20:
    - 'vmlinux.sh'
keywords_21:
    - 'bzImage'
keywords_22:
    - 'new_img'

keywords_23:
    - 'echo'
keywords_24:
    - 'awk'
keywords_25:
```

```
        - 'print'
    keywords_26:
        - 'output'

    condition: keywords or keywords_1 and keywords_2 or keywords_3 and keywords_4
or keywords_5 and keywords_6 and keywords_7 or keywords_8 and keywords_9 and
keywords_10 or keywords_11 and keywords_12 and keywords_13 or keywords_14 and
keywords_15 or keywords_16 and keywords_17 or keywords_18 and keywords_19 or
keywords_20 and keywords_21 and keywords_22 or keywords_23 and keywords_24 and
keywords_25 and keywords_26

falsepositives:
    - Rate of FP moderate with some strings.
    - Use this rule in an infected environment/logs.
    - Analyst may need to make adjustments to the query as required.
level: high
```