# CVE Detail – CVE-2020-28368

Xen through 4.14.x allows guest OS administrators to obtain sensitive information (such as AES keys from outside the guest) via a side-channel attack on a power/energy monitoring interface, aka a "Platypus" attack. NOTE: there is only one logically independent fix: to change the access control for each such interface in Xen.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.21016

## CVSS Scoring

CVSS v3.1 Score: 4.4

Severity: MEDIUM

## Mapped CWE(s)

* CWE-862: Missing Authorization

## CAPEC(s)

* CAPEC-665: Exploitation of Thunderbolt Protection Flaws

## ATT&CK Techniques

* T1542.002: Component Firmware
* T1556: Modify Authentication Process
* T1211: Exploitation for Defense Evasion

## Used By (Actors/Tools)

* Cyclops Blink (malware)
* Kessel (malware)
* Ebury (malware)
* SILENTTRINITY (tool)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Equation (intrusion-set)
* APT28 (intrusion-set)
* FIN13 (intrusion-set)

## Affected Products

* cpe:2.3:o:xen:xen:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:32:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:10.0:\*:\*:\*:\*:\*:\*:\*