# CVE Detail – CVE-2022-36349

Insecure default variable initialization in BIOS firmware for some Intel(R) NUC Boards and Intel(R) NUC Kits before version MYi30060 may allow an authenticated user to potentially enable denial of service via local access.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.18063

## CVSS Scoring

CVSS v3.1 Score: 5.2

Severity: MEDIUM

## Mapped CWE(s)

* CWE-1188: Initialization of a Resource with an Insecure Default

## 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:intel:nuc\_board\_nuc5i3mybe\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:intel:nuc\_kit\_nuc5i3myhe\_firmware:\*:\*:\*:\*:\*:\*:\*:\*