

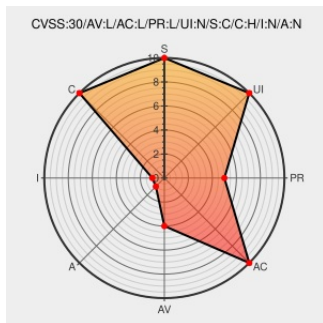


CVE-2020-13518

Published on: 12/17/2020 12:00:00 AM UTC

Last Modified on: 09/12/2022 06:37:00 PM UTC

CVE-2020-13518

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Cam](#) from [Nzxt](#) contain the following vulnerability:

An information disclosure vulnerability exists in the WinRing0x64 Driver IRP 0x9c402084 functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause the disclosure of sensitive information. An attacker can send a malicious IRP to trigger this vulnerability.

CVE-2020-13518 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	NONE	NONE

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
TALOS-2020-1115 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Technical Description Third Party Advisory talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2020-1115

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nzxt	Cam	4.8.0	All	All	All
Application	Nzxt	Cam	4.8.0	All	All	All
cpe:2.3:a:nzxt:cam:4.8.0:*:*:*:*:*:						
cpe:2.3:a:nzxt:cam:4.8.0:*:*:*:*:*:						

Social Mentions

Next ID→