



CVE-2017-5685

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2017-5685
State	PUBLIC
Assigner	secure@intel.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-03 21:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	The BIOS in Intel NUC systems based on 6th Gen Intel Core processors prior to version KY0045 may allow may allow an a

Risk And Classification

Problem Types: CWE-276

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Intel	Nuc6i7kyk	-	All	All	All
Hardware	Intel	Nuc6i7kyk	-	All	All	All
Operating System	Intel	Nuc6i7kyk Bios	kyskli70.86a.0042.2016.0929.1933	All	All	All
Operating System	Intel	Nuc6i7kyk Bios	kyskli70.86a.0042.2016.0929.1933	All	All	All

References

Reference	Source	Link	Tags
Intel® Product Security Center	CONFIRM	security-center.intel.com	Vendor Advis
Intel NUC and Compute Stick DCI Multiple Local Information Disclosure Vulnerabilities	BID	www.securityfocus.com	Third Party A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)