



CVE-2019-0365

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

Summary

CVE	CVE-2019-0365
State	PUBLIC
Assigner	cna@sap.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-10 17:15:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	SAP Kernel (RFC), KRNL32NUC, KRNL32UC and KRNL64NUC before versions 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64U

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Sap Kernel	7.21	All	All	All
Application	Sap	Sap Kernel	7.49	All	All	All
Application	Sap	Sap Kernel	7.53	All	All	All
Application	Sap	Sap Kernel	7.73	All	All	All
Application	Sap	Sap Kernel	7.76	All	All	All
Application	Sap	Sap Kernel	7.21	All	All	All
Application	Sap	Sap Kernel	7.49	All	All	All
Application	Sap	Sap Kernel	7.53	All	All	All
Application	Sap	Sap Kernel	7.73	All	All	All
Application	Sap	Sap Kernel	7.76	All	All	All
Application	Sap	Sap Kernel Krnl32nuc	7.21	All	All	All
Application	Sap	Sap Kernel Krnl32nuc	7.21ext	All	All	All
Application	Sap	Sap Kernel Krnl32nuc	7.22	All	All	All
Application	Sap	Sap Kernel Krnl32nuc	7.22ext	All	All	All
Application	Sap	Sap Kernel Krnl32nuc	7.21	All	All	All
Application	Sap	Sap Kernel Krnl32nuc	7.21ext	All	All	All
Application	Sap	Sap Kernel Krnl32nuc	7.22	All	All	All

Application	Sap	Sap Kernel Krnl32nuc	7.22ext	All	All	All
Application	Sap	Sap Kernel Krnl32uc	7.21	All	All	All
Application	Sap	Sap Kernel Krnl32uc	7.21ext	All	All	All
Application	Sap	Sap Kernel Krnl32uc	7.22	All	All	All
Application	Sap	Sap Kernel Krnl32uc	7.22ext	All	All	All
Application	Sap	Sap Kernel Krnl32uc	7.21	All	All	All
Application	Sap	Sap Kernel Krnl32uc	7.21ext	All	All	All
Application	Sap	Sap Kernel Krnl32uc	7.22	All	All	All
Application	Sap	Sap Kernel Krnl32uc	7.22ext	All	All	All
Application	Sap	Sap Kernel Krnl64nuc	7.21	All	All	All
Application	Sap	Sap Kernel Krnl64nuc	7.21ext	All	All	All
Application	Sap	Sap Kernel Krnl64nuc	7.22	All	All	All
Application	Sap	Sap Kernel Krnl64nuc	7.22ext	All	All	All
Application	Sap	Sap Kernel Krnl64nuc	7.21	All	All	All
Application	Sap	Sap Kernel Krnl64nuc	7.21ext	All	All	All
Application	Sap	Sap Kernel Krnl64nuc	7.22	All	All	All
Application	Sap	Sap Kernel Krnl64nuc	7.22ext	All	All	All
Application	Sap	Sap Kernel Krnl64uc	7.21	All	All	All
Application	Sap	Sap Kernel Krnl64uc	7.21ext	All	All	All
Application	Sap	Sap Kernel Krnl64uc	7.22	All	All	All
Application	Sap	Sap Kernel Krnl64uc	7.22ext	All	All	All
Application	Sap	Sap Kernel Krnl64uc	7.49	All	All	All
Application	Sap	Sap Kernel Krnl64uc	7.73	All	All	All
Application	Sap	Sap Kernel Krnl64uc	7.21	All	All	All
Application	Sap	Sap Kernel Krnl64uc	7.21ext	All	All	All
Application	Sap	Sap Kernel Krnl64uc	7.22	All	All	All
Application	Sap	Sap Kernel Krnl64uc	7.22ext	All	All	All
Application	Sap	Sap Kernel Krnl64uc	7.49	All	All	All
Application	Sap	Sap Kernel Krnl64uc	7.73	All	All	All

References						
Reference				Source	Link	Ta
SAP Security Patch Day – September 2019 - Product Security Response at SAP - SCN Wiki				CONFIRM	wiki.scn.sap.com	Ve
launchpad.support.sap.com				MISC	launchpad.support.sap.com	Pe
CVE Program record				CVE.ORG	www.cve.org	ca

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](#).

Free CVE JSON API [cve.report/api](#)

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