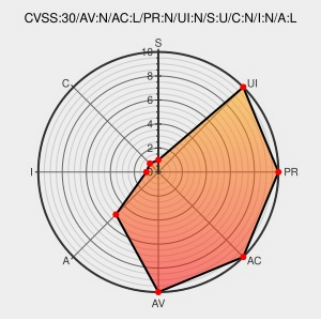
# CVE-2021-33684

Published on: 07/14/2021 12:00:00 AM UTC

Last Modified on: 07/27/2021 02:19:00 PM UTC

## CVE-2021-33684

Source: Mitre | Source: Nist | Print: PDF




Certain versions of Netweaver Abap from Sap contain the following vulnerability:

SAP NetWeaver AS ABAP and ABAP Platform, versions - KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, KRNL64UC 8.04, 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 8.04, 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.53, 7.77, 7.81, 7.84, allows an attacker to send overlong content in the RFC request type thereby crashing the corresponding work process because of memory corruption vulnerability. The work process will attempt to restart itself after the crash and hence the impact on the availability is low.

CVE-2021-33684 has been assigned by cna@sap.com to track the vulnerability - currently rated as MEDIUM severity.

### CVSS3 Score: 5.3 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | NONE | NONE | LOW |

### CVSS2 Score: 5 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | NONE | PARTIAL |

### CVE References

| Description | Tags | Link |
| --- | --- | --- |
| SAP Security Patch Day – July 2021 - Product Security Response at SAP - Community Wiki | wiki.scn.sap.com<br>text/html | MISC<br>wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=580617506 |
| No Description Provided | launchpad.support.sap.com<br>text/html | MISC<br>launchpad.support.sap.com/#/notes/3032624 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
| --- | --- | --- | --- | --- | --- | --- |
| Application | Sap | Netweaver Abap | 7.21 | All | All | All |
| Application | Sap | Netweaver Abap | 7.21ext | All | All | All |
| Application | Sap | Netweaver Abap | 7.22 | All | All | All |
| Application | Sap | Netweaver Abap | 7.22ext | All | All | All |
| Application | Sap | Netweaver Abap | 7.49 | All | All | All |
| Application | Sap | Netweaver Abap | 7.53 | All | All | All |
| Application | Sap | Netweaver Abap | 7.77 | All | All | All |
| Application | Sap | Netweaver Abap | 7.81 | All | All | All |
| Application | Sap | Netweaver Abap | kernel_8.04 | All | All | All |
| Application | Sap | Netweaver Abap | krnl32nuc_7.21 | All | All | All |
| Application | Sap | Netweaver Abap | krnl32uc_7.21 | All | All | All |
| Application | Sap | Netweaver Abap | krnl64nuc_7.21 | All | All | All |
| Application | Sap | Netweaver Abap | krnl64uc_8.04 | All | All | All |
| Application | Sap | Netweaver As Abap | 7.21 | All | All | All |
| Application | Sap | Netweaver As Abap | 7.21ext | All | All | All |
| Application | Sap | Netweaver As Abap | 7.22 | All | All | All |
| Application | Sap | Netweaver As Abap | 7.22ext | All | All | All |
| Application | Sap | Netweaver As Abap | 7.49 | All | All | All |
| Application | Sap | Netweaver As Abap | 7.53 | All | All | All |
| Application | Sap | Netweaver As Abap | 7.77 | All | All | All |
| Application | Sap | Netweaver As Abap | 7.81 | All | All | All |
| Application | Sap | Netweaver As Abap | kernel_8.04 | All | All | All |
| Application | Sap | Netweaver As Abap | krnl32nuc_7.21 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Sap | Netweaver As Abap | krnl32uc_7.21 | All | All | All |
| Application | Sap | Netweaver As Abap | krnl64nuc_7.21 | All | All | All |
| Application | Sap | Netweaver As Abap | krnl64uc_8.04 | All | All | All |

cpe:2.3:a:sap:netweaver_abap:7.21:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_abap:7.21ext:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_abap:7.22:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_abap:7.22ext:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_abap:7.49:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_abap:7.53:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_abap:7.77:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_abap:7.81:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_abap:kernel_8.04:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_abap:krnl32nuc_7.21:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_abap:krnl32uc_7.21:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_abap:krnl64nuc_7.21:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_abap:krnl64uc_8.04:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:7.21:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:7.21ext:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:7.22:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:7.22ext:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:7.49:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:7.53:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:7.77:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:7.81:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:kernel_8.04:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:krnl32nuc_7.21:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:krnl32uc_7.21:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:krnl64nuc_7.21:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:krnl64uc_8.04:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @CVEreport | CVE-2021-33684 : #SAP NetWeaver AS ABAP and ABAP Platform, versions - KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL3… twitter.com/i/web/status/1… | 2021-07-14 11:46:52 |
| /r/netcve | CVE-2021-33684 | 2021-07-14 12:41:22 |

← Previous ID

Next ID→