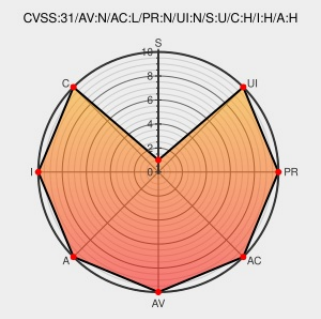
# CVE-2011-1180

Published on: 06/08/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:15 PM UTC

## CVE-2011-1180

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Linux Kernel from Linux contain the following vulnerability:

Multiple stack-based buffer overflows in the iriap_getvaluebyclass_indication function in net/irda/iriap.c in the Linux kernel before 2.6.39 allow remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging connectivity to an IrDA infrared network and sending a large integer value for a (1) name length or (2) attribute length.

CVE-2011-1180 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as CRITICAL severity.

### CVSS3 Score: 9.8 - CRITICAL

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

### CVSS2 Score: 7.5 - HIGH

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

### CVE References

| Description | Tags | Link |
|---|---|---|
| irda: validate peer name and attribute lengths · | Third Party Advisory<br>github.com | CONFIRM<br>github.com/torvalds/linux/commit/d370af0ef7951188daeb15bae75db7ba57c67846 |

| | | |
|---|---|---|
| torvalds/linux@d370af0 · GitHub | text/html | |
| oss-security - Re: CVE requests - kernel: irda/decnet issues | Mailing List<br>Third Party Advisory<br>www.openwall.com<br>text/html | MLIST [oss-security] 20110322 Re: CVE requests - kernel: irda/decnet issues |
| kernel/git/torvalds/linux.git - Linux kernel source tree | Patch<br>Vendor Advisory<br>git.kernel.org<br>text/html | CONFIRM git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=d370af0ef7951188daeb15bae75db7ba57c67846 |
| 404 Not Found | Release Notes<br>Third Party Advisory<br>ftp.osuosl.org<br>text/plain<br>Inactive Link Not Archived | CONFIRM ftp.osuosl.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→