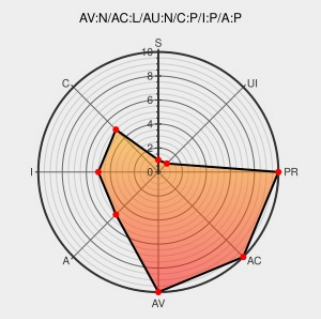
CVE-2014-8154

Published on: 01/27/2015 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:10 AM UTC

CVE-2014-8154

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



Certain versions of Vala from Gnome contain the following vulnerability:

The Gst.MapInfo function in Vala 0.26.0 and 0.26.1 uses an incorrect buffer length declaration for the Gstreamer bindings, which allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via unspecified vectors, which trigger a heap-based buffer overflow.

CVE-2014-8154 has been assigned by secalert@redhat.com to track the vulnerability

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
Bug 1181404 – CVE-2014-8154 Vala: Heap-buffer overflow in vala-gstreamer bindings at Gst.MapInfo()	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1181404
openSUSE-SU-2015:0131-1: moderate: Security update for shotwell, vala	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:0131
1177840 – All Vala programs that use Gst.MapInfo() are vulnerable to heap buffer overflow due to a bug in Vala bindings for GStreamer	Patch bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1177840

comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnome	Vala	0.26.0	All	All	All
Application	Gnome	Vala	0.26.1	All	All	All
Application	Gnome	Vala	0.26.0	All	All	All
Application	Gnome	Vala	0.26.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All

cpe:2.3:a:gnome:vala:0.26.0:*:*:*:*:*:*:*:

cpe:2.3:a:gnome:vala:0.26.1:*:*:*:*:*:*:*:

cpe:2.3:a:gnome:vala:0.26.0:*:*:*:*:*:*:*:

cpe:2.3:a:gnome:vala:0.26.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→