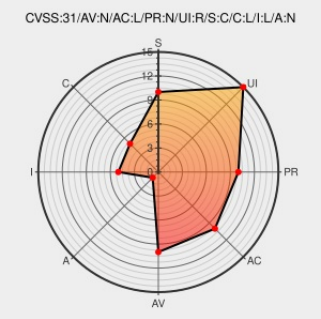
CVE-2014-10400

Published on: 02/06/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:45 PM UTC

CVE-2014-10400

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



Certain versions of Cgilua from Keplerproject contain the following vulnerability:

The session.lua library in CGILua 5.0.x uses sequential session IDs, which makes it easier for remote attackers to predict the session ID and hijack arbitrary sessions. NOTE: this vulnerability was SPLIT from CVE-2014-2875.

CVE-2014-10400 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
No Description Provided	Third Party Advisory www.syhunt.com text/html	MISC www.syhunt.com/en/index.php?n=Advisories.Cgilua-weaksessionid
Full Disclosure: Syhunt Advisory: CGILua	Mailing List	MISC seclists.org/fulldisclosure/2014/Apr/318

session.lua Predictable Session ID Vulnerability	Third Party Advisory seclists.org text/html	
SecurityFocus	Third Party Advisory VDB Entry web.archive.org text/html Inactive Link Not Archived	MISC www.securityfocus.com/archive/1/531981/100/0/threaded

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to 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	Keplerproject	Cgilua	5.2	alpha1	All	All
Application	Keplerproject	Cgilua	5.2	alpha2	All	All
Application	Keplerproject	Cgilua	5.2	alpha1	All	All
Application	Keplerproject	Cgilua	5.2	alpha2	All	All
Application	Keplerproject	Cgilua	All	All	All	All
Application	Keplerproject	Cgilua	All	All	All	All

cpe:2.3:a:keplerproject:cgilua:5.2:alpha1:*:*:*:*:*:*:

cpe:2.3:a:keplerproject:cgilua:5.2:alpha2:*:*:*:*:*:*:

cpe:2.3:a:keplerproject:cgilua:5.2:alpha1:*:*:*:*:*:*:

cpe:2.3:a:keplerproject:cgilua:5.2:alpha2:*:*:*:*:*:*:

cpe:2.3:a:keplerproject:cgilua:*:*:*:*:*:*:*:*:

cpe:2.3:a:keplerproject:cgilua:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report