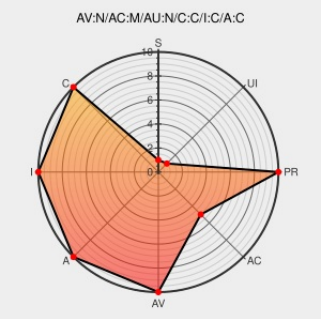
CVE-2011-3503

Published on: 09/16/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:13 PM UTC

CVE-2011-3503

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



Certain versions of Esignal from Interactivedata contain the following vulnerability:

Untrusted search path vulnerability in eSignal 10.6.2425.1208, and possibly other versions, allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse JRS_UT.dll that is located in the same folder as a .quo (QUOTE) file. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.

CVE-2011-3503 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 9.3 - HIGH

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF esignal-dll-code-execution(69786)
eSignal Buffer Overflow and Insecure Library Loading Vulnerabilities - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 45966
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 75458

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

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	Interactivedata	Esignal	10.6.2425.1208	All	All	All
Application	Interactivedata	Esignal	10.6.2425.1208	All	All	All

cpe:2.3:a:interactivedata:esignal:10.6.2425.1208:*:*:*:*:*:*:*:

cpe:2.3:a:interactivedata:esignal:10.6.2425.1208:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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