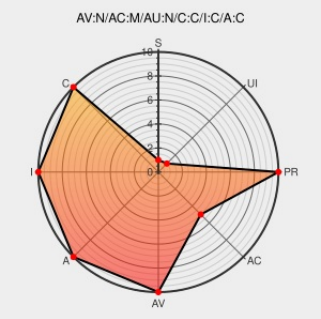
CVE-2010-2991

Published on: 08/11/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:09 PM UTC

CVE-2010-2991

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



Certain versions of Online Plug-in For Windows For Xenapp Xendesktop from Citrix contain the following vulnerability:

The IICAClient interface in the ICAClient library in the ICA Client ActiveX Object (aka ICO) component in Citrix Online Plug-in for Windows for XenApp & XenDesktop before 12.0.3 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted HTML document that triggers the reading of a .ICA file.

CVE-2010-2991 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
Citrix XenApp Online Plug-in ActiveX Control Code Execution Vulnerability - Advisories - Community	Vendor Advisory, web.archive.org, text/html	SECUNIA 40819
Vulnerability in Citrix XenApp Online Plug-in for Windows Could Result in Arbitrary Code Execution	Patch, Vendor Advisory, support.citrix.com, text/html	CONFIRM support.citrix.com/article/CTX125976
Citrix XenApp Online Plug-in ActiveX Control Code Execution Vulnerability - Secunia.com	Vendor Advisory, web.archive.org, text/html	SECUNIA 40821
Public Advisory: 08.03.10 // iDefense Labs	web.archive.org	IDEFENSE 20100803 Citrix ICA Client

text/html
Inactive Link Not Archived

ActiveX Memory Corruption Vulnerabillity

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	Citrix	Online Plug-in For Windows For Xenapp Xendesktop	11.1	All	All	All
Application	Citrix	Online Plug-in For Windows For Xenapp Xendesktop	All	All	All	All
Application	Citrix	Online Plug-in For Windows For Xenapp Xendesktop	11.1	All	All	All
Application	Citrix	Online Plug-in For Windows For Xenapp Xendesktop	11.1	All	All	All
Application	Citrix	Online Plug-in For Windows For Xenapp Xendesktop	All	All	All	All

cpe:2.3:a:citrix:online_plug-in_for_windows_for_xenapp_&_xendesktop:11.1:*:*:*:*:*:*:*:

cpe:2.3:a:citrix:online_plug-in_for_windows_for_xenapp_&_xendesktop:*:*:*:*:*:*:*:*:

cpe:2.3:a:citrix:online_plug-in_for_windows_for_xenapp_\&_xendesktop:11.1:*:*:*:*:*:*:*:

cpe:2.3:a:citrix:online_plug-in_for_windows_for_xenapp_\&_xendesktop:11.1:*:*:*:*:*:*:*:

cpe:2.3:a:citrix:online_plug-in_for_windows_for_xenapp_\&_xendesktop:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→