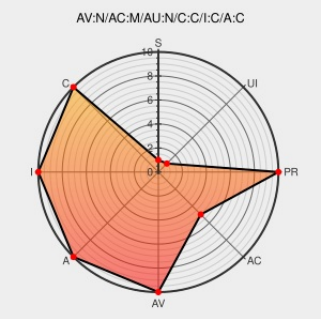
CVE-2011-2882

Published on: 07/21/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:20 PM UTC

CVE-2011-2882

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



Certain versions of Access Gateway from Citrix contain the following vulnerability:

Stack-based buffer overflow in the NSEPA.NsepaCtrl.1 ActiveX control in nsepa.ocx in Citrix Access Gateway Enterprise Edition 8.1 before 8.1-67.7, 9.0 before 9.0-70.5, and 9.1 before 9.1-96.4 allows remote attackers to execute arbitrary code via crafted HTTP header data.

CVE-2011-2882 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 Gateway ActiveX Control Stack Based Buffer Overflow Vulnerability - CXSecurity.com	securityreason.com text/html	SREASON 8358
No Description Provided	labs.idefense.com Inactive Link Not Archived	IDEFENSE 20110714 Citrix Access Gateway ActiveX Stack Buffer Overflow Vulnerability

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Citrix	Access Gateway	8.1	All	enterprise	All
Application	Citrix	Access Gateway	9.0	All	enterprise	All
Application	Citrix	Access Gateway	9.1	All	enterprise	All
Application	Citrix	Access Gateway	8.1	All	enterprise	All
Application	Citrix	Access Gateway	9.0	All	enterprise	All
Application	Citrix	Access Gateway	9.1	All	enterprise	All

cpe:2.3:a:citrix:access_gateway:8.1:*:enterprise:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:9.0:*:enterprise:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:9.1:*:enterprise:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:8.1:*:enterprise:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:9.0:*:enterprise:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:9.1:*:enterprise:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→