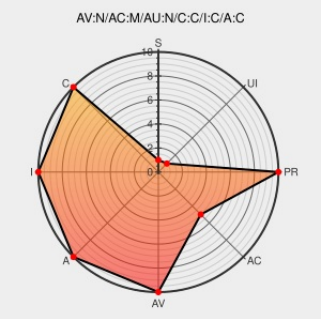
CVE-2010-4566

Published on: 01/14/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:00 PM UTC

CVE-2010-4566

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



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

The web authentication form in the NT4 authentication component in Citrix Access Gateway Enterprise Edition 9.2-49.8 and earlier, and the NTLM authentication component in Access Gateway Standard and Advanced Editions before Access Gateway 5.0, allows attackers to execute arbitrary commands via shell metacharacters in the password field.

CVE-2010-4566 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
VSR Security Advisories	web.archive.org text/html Inactive Link Not Archived	MISC www.vsecurity.com/resources/advisory/20101221-1
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 70099
Vulnerability in Citrix Access Gateway legacy authentication support could result in command injection	Vendor Advisory support.citrix.com text/html	CONFIRM support.citrix.com/article/CTX127613
Citrix Access Gateway Command Execution - SecurityReason.com	securityreason.com text/html	SREASON 8119

SecurityTracker: Citrix Access Gateway Flaw in Legacy NT Authentication Component Lets Remote Users Inject Commands	www.securitytracker.com text/html	SECTRACK 1024893
Citrix Access Gateway Command Execution	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 16916

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	.8.0	m50.3	enterprise	All
Application	Citrix	Access Gateway	4.5	All	advanced	All
Application	Citrix	Access Gateway	4.5	All	standard	All
Application	Citrix	Access Gateway	4.5	hf1	All	All
Application	Citrix	Access Gateway	4.5	hf1	advanced	All
Application	Citrix	Access Gateway	4.5.5	All	standard	All
Application	Citrix	Access Gateway	4.5.6	All	standard	All
Application	Citrix	Access Gateway	4.5.7	All	standard	All
Application	Citrix	Access Gateway	4.6.1	All	standard	All
Application	Citrix	Access Gateway	4.6.2	All	standard	All
Application	Citrix	Access Gateway	4.6.3	All	standard	All
Application	Citrix	Access Gateway	8.0	m48.7	enterprise	All
Application	Citrix	Access Gateway	8.0	m49.2	enterprise	All
Application	Citrix	Access Gateway	8.0	m59.1	enterprise	All
Application	Citrix	Access Gateway	8.1-69.4	All	enterprise	All
Application	Citrix	Access Gateway	9.0.71.3	All	enterprise	All
Application	Citrix	Access Gateway	9.1-104.5	All	enterprise	All
Application	Citrix	Access Gateway	.8.0	m50.3	enterprise	All
Application	Citrix	Access Gateway	4.5	All	advanced	All
Application	Citrix	Access Gateway	4.5	All	standard	All
Application	Citrix	Access Gateway	4.5	hf1	All	All
Application	Citrix	Access Gateway	4.5	hf1	advanced	All
Application	Citrix	Access Gateway	4.5.5	All	standard	All

Application	Citrix	Access Gateway	4.5.6	All	standard	All
Application	Citrix	Access Gateway	4.5.7	All	standard	All
Application	Citrix	Access Gateway	4.6.1	All	standard	All
Application	Citrix	Access Gateway	4.6.2	All	standard	All
Application	Citrix	Access Gateway	4.6.3	All	standard	All
Application	Citrix	Access Gateway	8.0	m48.7	enterprise	All
Application	Citrix	Access Gateway	8.0	m49.2	enterprise	All
Application	Citrix	Access Gateway	8.0	m59.1	enterprise	All
Application	Citrix	Access Gateway	8.1-69.4	All	enterprise	All
Application	Citrix	Access Gateway	9.0.71.3	All	enterprise	All
Application	Citrix	Access Gateway	9.1-104.5	All	enterprise	All
Application	Citrix	Access Gateway	All	All	enterprise	All

cpe:2.3:a:citrix:access_gateway:.8.0:m50.3:enterprise:*:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.5:*:advanced:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.5:*:standard:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.5:hf1:*:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.5:hf1:advanced:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.5.5:*:standard:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.5.6:*:standard:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.5.7:*:standard:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.6.1:*:standard:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.6.2:*:standard:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.6.3:*:standard:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:8.0:m48.7:enterprise:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:8.0:m49.2:enterprise:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:8.0:m59.1:enterprise:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:8.1-69.4:*:enterprise:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:9.0.71.3:*:enterprise:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:9.1-104.5:*:enterprise:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:.8.0:m50.3:enterprise:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.5:*:advanced:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.5:*:standard:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.5:hf1:*:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.5:hf1:advanced:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.5.5:*:standard:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.5.6:*:standard:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.5.7:*:standard:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.6.1:*:standard:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.6.2:*:standard:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:4.6.3:*:standard:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:8.0:m48.7:enterprise:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:8.0:m49.2:enterprise:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:8.0:m59.1:enterprise:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:8.1-69.4:*:enterprise:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:9.0.71.3:*:enterprise:*:*:*:*:*:

cpe:2.3:a:citrix:access_gateway:9.1-104.5:*:enterprise:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→