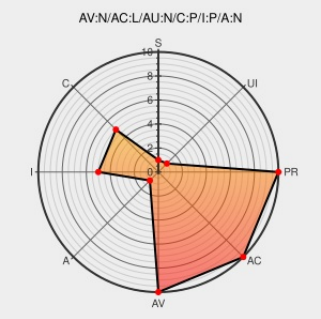
CVE-2001-1568

Published on: 12/31/2001 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:19 PM UTC

CVE-2001-1568

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



Certain versions of Wap Gateway from Cmg contain the following vulnerability:

CMG WAP gateway does not verify the fully qualified domain name URL with X.509 certificates from root certificate authorities, which allows remote attackers to spoof SSL certificates via a man-in-the-middle attack.

CVE-2001-1568 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
Neohapsis Archives - Bugtraq - Many WAP gateways do not properly check SSL certificates - From angus@z-y-g-o.com	web.archive.org, text/html, Inactive Link, Not Archived	BUGTRAQ 20010709 Many WAP gateways do not properly check SSL certificates
ISS X-Force Database:	web.archive.org, text/html, Inactive Link, Not Archived	XF wap-gateway-ssl-certificates(6814)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cmg	Wap Gateway	All	All	All	All
Application	Cmg	Wap Gateway	All	All	All	All

cpe:2.3:a:cmg:wap_gateway:*:*:*:*:*:*:*:*:

cpe:2.3:a:cmg:wap_gateway:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→