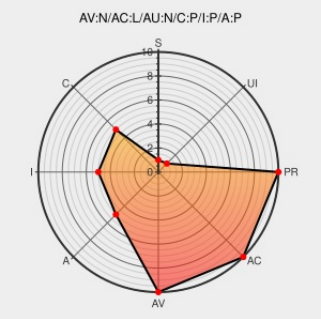
CVE-2013-1337

Published on: 05/14/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:32 PM UTC

CVE-2013-1337

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



Certain versions of .net Framework from Microsoft contain the following vulnerability:

Microsoft .NET Framework 4.5 does not properly create policy requirements for custom Windows Communication Foundation (WCF) endpoint authentication in certain situations involving passwords over HTTPS, which allows remote attackers to bypass authentication by sending queries to an endpoint, aka "Authentication Bypass Vulnerability."

CVE-2013-1337 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Microsoft Updates for Multiple Vulnerabilities | US-CERT	Third Party Advisory, US Government Resource, www.us-cert.gov, text/html	CERT TA13-134A
Microsoft Security Bulletin MS13-040 - Important | Microsoft Docs	docs.microsoft.com, text/html	MS MS13-040
Repository / Oval Repository	oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:16741

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	Microsoft	.net Framework	4.5	All	All	All
Application	Microsoft	.net Framework	4.5	All	All	All

cpe:2.3:a:microsoft:.net_framework:4.5:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:4.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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