



# CVE-2011-1889

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2011-1889
<b>State</b>	PUBLIC
<b>Assigner</b>	secure@microsoft.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2011-06-16 20:55:00 UTC
<b>Updated</b>	2018-10-12 22:01:00 UTC
<b>Description</b>	The NSPLookupServiceNext function in the client in Microsoft Forefront Threat Management Gateway (TMG) 2010 allows r

## Risk And Classification

**EPSS:** 0.853530000 probability, percentile 0.993580000 (date 2026-04-02)

**CISA KEV:** Listed on 2022-03-03; due 2022-03-24; ransomware use Unknown

**Problem Types:** CWE-119

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Microsoft
<b>Product</b>	Forefront Threat Management Gateway (TMG)
<b>Name</b>	Microsoft Forefront TMG Remote Code Execution Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2011-1889">https://nvd.nist.gov/vuln/detail/CVE-2011-1889</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Microsoft</a>	<a href="#">Forefront Threat Management Gateway</a>	2010	All	All	All
Application	<a href="#">Microsoft</a>	<a href="#">Forefront Threat Management Gateway</a>	2010	All	All	All

## References

Reference
Microsoft Forefront Threat Management Gateway Bounds Validation Flaw in Winsock Provider Lets Remote Users Execute Arbitrary Code - S
IBM X-Force Exchange
Repository / Oval Repository

Microsoft Threat Management Gateway Firewall Client Vulnerability - Secunia.com

Microsoft Forefront Threat Management Gateway (TMG) Firewall Client Memory Corruption Vulnerability

Microsoft Security Bulletin MS11-040 - Critical | Microsoft Docs

CVE Program record

NVD vulnerability detail

CISA Known Exploited Vulnerabilities catalog



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**