



CVE-2010-3332

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2010-3332
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-09-22 19:00:00 UTC
Updated	2020-11-23 19:50:00 UTC
Description	Microsoft .NET Framework 1.1 SP1, 2.0 SP1 and SP2, 3.5, 3.5 SP1, 3.5.1, and 4.0, as used for ASP.NET in Microsoft Inter

Risk And Classification

Problem Types: CWE-209

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	.net Framework	1.1	sp1	All	All
Application	Microsoft	.net Framework	2.0	sp1	All	All
Application	Microsoft	.net Framework	2.0	sp2	All	All
Application	Microsoft	.net Framework	3.5	-	All	All
Application	Microsoft	.net Framework	3.5	sp1	All	All
Application	Microsoft	.net Framework	3.5.1	All	All	All
Application	Microsoft	.net Framework	4.0	-	All	All
Application	Microsoft	.net Framework	1.1	sp1	All	All
Application	Microsoft	.net Framework	2.0	sp1	All	All
Application	Microsoft	.net Framework	2.0	sp2	All	All
Application	Microsoft	.net Framework	3.5	-	All	All
Application	Microsoft	.net Framework	3.5	sp1	All	All
Application	Microsoft	.net Framework	3.5.1	All	All	All
Application	Microsoft	.net Framework	4.0	-	All	All
Application	Microsoft	Internet Information Services	-	All	All	All
Application	Microsoft	Internet Information Services	-	All	All	All

References

Reference	Source	Link
ekoparty Security Conference	MISC	www.ekoparty.c
Important: ASP.NET Security Vulnerability - ScottGu's Blog	CONFIRM	weblogs.asp.ne
DotNetNuke Blogs - Oracle Padding Vulnerability in ASP.NET	MISC	www.dotnetnuk
JavaScript is not available.	MISC	twitter.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.cor
Understanding the ASP.NET Vulnerability - Security Research & Defense - Site Home - TechNet Blogs	CONFIRM	blogs.technet.c
Microsoft Security Bulletin MS10-070 - Important Microsoft Docs	MS	docs.microsoft.i
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.cor
Repository / Oval Repository	OVAL	oval.cisecurity.c
Your request has been blocked. This could be due to several reasons.	CONFIRM	www.microsoft.
Vulnerabilities - Mono	CONFIRM	www.mono-proj
Microsoft .NET Framework ASP.NET Padding Oracle Information Disclosure Vulnerability	BID	www.securityfo
ASP.NET POET Vulnerability - What Else Can I Do? : The Penton-izer	MISC	pentonizer.com
Security researchers 'destroy' microsoft asp.net security - The Inquirer	MISC	www.theinquire
InfoSec Handlers Diary Blog	MISC	isc.sans.edu
Troy Hunt: Fear, uncertainty and the padding oracle exploit in ASP.NET	MISC	www.troyhunt.c
SecurityTracker.com Archives - Microsoft ASP.NET Padding Oracle Attack Lets Remote Users Decrypt Data	SECTRACK	securitytracker.
IBM X-Force Exchange	XF	exchange.xforc
'Padding Oracle' Crypto Attack Affects Millions of ASP.NET Apps threatpost	MISC	threatpost.com
Microsoft ASP.NET Cryptographic Padding Oracle Information Disclosure - Advisories - Community	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/).

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