



CVE-2014-4122

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-4122
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-15 10:55:00 UTC
Updated	2018-10-12 22:07:00 UTC
Description	Microsoft .NET Framework 2.0 SP2, 3.5, and 3.5.1 omits the ASLR protection mechanism, which allows remote attackers to

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	.net Framework	2.0	sp2	All	All
Application	Microsoft	.net Framework	3.5	All	All	All
Application	Microsoft	.net Framework	3.5.1	All	All	All
Application	Microsoft	.net Framework	2.0	sp2	All	All
Application	Microsoft	.net Framework	3.5	All	All	All
Application	Microsoft	.net Framework	3.5.1	All	All	All

References

Reference	Source	Link
Microsoft Security Bulletin MS14-057 - Critical Microsoft Docs	MS	do
About Secunia Research Flexera	SECUNIA	se
Microsoft .NET Framework CVE-2014-4122 ASLR Security Bypass Vulnerability	BID	wv
Microsoft .NET Bugs Let Remote Users Bypass ASLR Security Protections and Execute Arbitrary Code - SecurityTracker	SECTRACK	wv
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv

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](#).

Free CVE JSON API [cve.report/api](#)

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