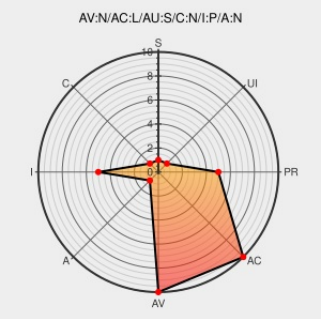
CVE-2006-1510

Published on: 03/29/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:01 PM UTC

CVE-2006-1510

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



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

Buffer overflow in calloc.c in the Microsoft Windows XP SP2 ntdll.dll system library, when used by the ILDASM disassembler in the Microsoft .NET 1.0 and 1.1 SDK, might allow user-assisted attackers to execute arbitrary code via a crafted .dll file with a large static method.

CVE-2006-1510 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Owasp .Net - To MSRC: Buffer OverFlow in ILASM and ILDASM	Exploit, owasp.net, text/html	MISC owasp.net/forums/257/showpost.aspx
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF ms-dotnet-ildasm-bo(25439)
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com, text/html	VUPEN ADV-2006-1113
Microsoft .NET Framework SDK MSIL Tools Buffer Overflow Vulnerabilities	Exploit, Patch, cve.report (archive), text/html	BID 17243
[Full-disclosure] Buffer OverFlow in ILASM and ILDASM	Exploit, Patch	FULLDISC 20060327 Buffer OverFlow in ILASM and ILDASM

	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	
OWASP Foundation | Open Source Foundation for Application Security	Exploit Patch owasp.net text/html	MISC owasp.net/forums/234/showpost.aspx
Microsoft .NET Framework SDK ildasm Buffer Overflow - Advisories - Secunia	Exploit Patch Vendor Advisory web.archive.org text/html	SECUNIA 19406

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	1.0	All	All	All
Application	Microsoft	.net Framework	1.0	sp1	sdk	All
Application	Microsoft	.net Framework	1.0	sp2	sdk	All
Application	Microsoft	.net Framework	1.1	All	All	All
Application	Microsoft	.net Framework	1.1	sp1	sdk	All
Application	Microsoft	.net Framework	1.0	All	All	All
Application	Microsoft	.net Framework	1.0	sp1	sdk	All
Application	Microsoft	.net Framework	1.0	sp2	sdk	All
Application	Microsoft	.net Framework	1.1	All	All	All
Application	Microsoft	.net Framework	1.1	sp1	sdk	All

cpe:2.3:a:microsoft:.net_framework:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:1.0:sp1:sdk:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:1.0:sp2:sdk:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:1.1:sp1:sdk:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:1.0:sp1:sdk:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:1.0:sp2:sdk:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:.net_framework:1.1:sp1:sdk:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→