



CVE-2005-2482

Published on: 08/07/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

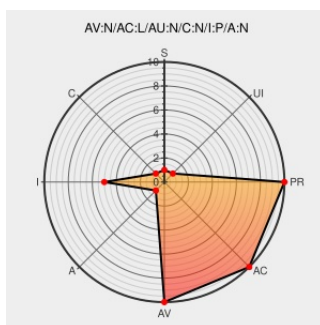
CVE-2005-2482

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Metasploit Framework](#) from [Metasploit](#) contain the following vulnerability:

The StateToOptions function in msfweb in Metasploit Framework 2.4 and earlier, when running with the -D option (defanged mode), allows attackers to modify temporary environment variables before the "_Defanged" environment option is checked when processing the Exploit command.

CVE-2005-2482 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

[framework] msfweb "refang" security update

[web.archive.org](#)

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[CONFIRM](#)
[metasploit.com/archive/framework/msg00469.html](#)

Secunia - Advisories - Metasploit Framework
"defanged" Mode Bypass Vulnerability

[Patch](#)

[Vendor Advisory](#)

[web.archive.org](#)

[text/html](#)

[SECUNIA 16318](#)

Metasploit Framework MSFWeb Defanged Mode
Restriction Bypass Vulnerability

[cve.report \(archive\)](#)

[text/html](#)

[BID 14455](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)

[text/html](#)

[XF metasploit-defanged-bypass-security\(21705\)](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that 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	Metasploit	Metasploit Framework	2.0	All	All	All
Application	Metasploit	Metasploit Framework	2.1	All	All	All
Application	Metasploit	Metasploit Framework	2.2	All	All	All
Application	Metasploit	Metasploit Framework	2.3	All	All	All
Application	Metasploit	Metasploit Framework	2.4	All	All	All
Application	Metasploit	Metasploit Framework	2.0	All	All	All
Application	Metasploit	Metasploit Framework	2.1	All	All	All
Application	Metasploit	Metasploit Framework	2.2	All	All	All
Application	Metasploit	Metasploit Framework	2.3	All	All	All
Application	Metasploit	Metasploit Framework	2.4	All	All	All

cpe:2.3:a:metasploit:metasploit_framework:2.0:*:*:*:*:*:

cpe:2.3:a:metasploit:metasploit_framework:2.1:*:*:*:*:*:

cpe:2.3:a:metasploit:metasploit_framework:2.2:*:*:*:*:*:

cpe:2.3:a:metasploit:metasploit_framework:2.3:*:*:*:*:*:

cpe:2.3:a:metasploit:metasploit_framework:2.4:*:*:*:*:*:

cpe:2.3:a:metasploit:metasploit_framework:2.0:*:*:*:*:*:

cpe:2.3:a:metasploit:metasploit_framework:2.1:*:*:*:*:*:

cpe:2.3:a:metasploit:metasploit_framework:2.2:*:*:*:*:*:

cpe:2.3:a:metasploit:metasploit_framework:2.3:*:*:*:*:*:

cpe:2.3:a:metasploit:metasploit_framework:2.4:*:*:*:*:*:

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

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](#)