

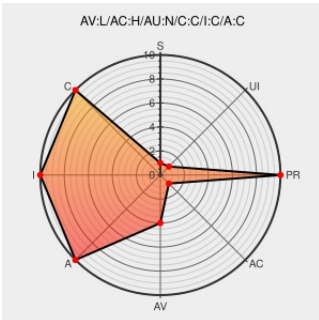


CVE-2011-1056

Published on: 02/21/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:15 PM UTC

CVE-2011-1056

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

The installer for Metasploit Framework 3.5.1, when running on Windows, uses weak inherited permissions for the Metasploit installation directory, which allows local users to gain privileges by replacing critical files with a Trojan horse.

CVE-2011-1056 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.2 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

HIGH

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Metasploit Framework Insecure Filesystem Permissions
Security Issue - Advisories - Community

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[X](#) [SECUNIA 43166](#)

Webmail : Solution de messagerie professionnelle - OVHcloud-
OVH

[Vendor Advisory](#)
[www.vupen.com](#)
[text/html](#)

[VUPEN ADV-2011-0371](#)

Rapid7 Community: Community: Metasploit

[blog.metasploit.com](#)
[text/html](#)

[CONFIRM](#)
[blog.metasploit.com/2011/02/metasploit-framework-352-released.html](#)

No Description Provided

[osvdb.org](#)

[OSVDB 70857](#)

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

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

By clicking these links, you may be leaving CVEreport website. 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	3.5.1	All	All	All
Application	Metasploit	Metasploit Framework	3.5.1	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
cpe:2.3:a:metasploit:metasploit_framework:3.5.1:*:*:*:*:*:						
cpe:2.3:a:metasploit:metasploit_framework:3.5.1:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows.*:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows.*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© 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