



CVE-2013-4986

Published on: 10/04/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:29 PM UTC

CVE-2013-4986

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

Certain versions of Pdfcool Studio from Iconcool contain the following vulnerability:

Stack-based buffer overflow in PDFAX0722_IconCool.dll 7.22.1125.2121 in IconCool PDFCool Studio 3.32 Build 130330 and earlier allows remote attackers to execute arbitrary code via a crafted PDF file.

CVE-2013-4986 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

PDFCool Studio Buffer Overflow Vulnerability | CORE Security

Exploit

www.coresecurity.com

[text/html](#)

MISC

www.coresecurity.com/advisories/pdfcool-studio-buffer-overflow-vulnerability

No Description Provided

Exploit

archives.neohapsis.com

BUGTRAQ 20131001 CORE-2013-0828 - PDFCool Studio Buffer Overflow Vulnerability

Inactive Link

Not Archived

No Description Provided

osvdb.org

OSVDB 97959

Inactive Link

Not Archived

PDFCool Studio Buffer Overflow ~ Packet Storm

Exploit

packetstormsecurity.com

[text/html](#)

MISC

packetstormsecurity.com/files/123476

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	Iconcool	Pdfcool Studio	2.0	build110427	All	All
Application	Iconcool	Pdfcool Studio	2.0	build110502	All	All
Application	Iconcool	Pdfcool Studio	2.0	build110508	All	All
Application	Iconcool	Pdfcool Studio	2.0	build110510	All	All
Application	Iconcool	Pdfcool Studio	2.0	build110512	All	All
Application	Iconcool	Pdfcool Studio	2.10	build110519	All	All
Application	Iconcool	Pdfcool Studio	2.10	build110523	All	All
Application	Iconcool	Pdfcool Studio	2.12	build110528	All	All
Application	Iconcool	Pdfcool Studio	2.14	build110608	All	All
Application	Iconcool	Pdfcool Studio	2.16	build110612	All	All
Application	Iconcool	Pdfcool Studio	2.20	build110707	All	All
Application	Iconcool	Pdfcool Studio	2.24	build1110801	All	All
Application	Iconcool	Pdfcool Studio	2.26	build110823	All	All
Application	Iconcool	Pdfcool Studio	2.30	build110920	All	All
Application	Iconcool	Pdfcool Studio	2.40	build111016	All	All
Application	Iconcool	Pdfcool Studio	2.5	build120405	All	All
Application	Iconcool	Pdfcool Studio	2.6	build120405	All	All
Application	Iconcool	Pdfcool Studio	2.7	build120405	All	All
Application	Iconcool	Pdfcool Studio	2.8	build120518	All	All
Application	Iconcool	Pdfcool Studio	3.0	build121022	All	All
Application	Iconcool	Pdfcool Studio	2.0	build110427	All	All
Application	Iconcool	Pdfcool Studio	2.0	build110502	All	All
Application	Iconcool	Pdfcool Studio	2.0	build110508	All	All
Application	Iconcool	Pdfcool Studio	2.0	build110510	All	All
Application	Iconcool	Pdfcool Studio	2.0	build110512	All	All
Application	Iconcool	Pdfcool Studio	2.10	build110519	All	All

Application	Iconcool	Pdfcool Studio	2.10	build110523	All	All
Application	Iconcool	Pdfcool Studio	2.12	build110528	All	All
Application	Iconcool	Pdfcool Studio	2.14	build110608	All	All
Application	Iconcool	Pdfcool Studio	2.16	build110612	All	All
Application	Iconcool	Pdfcool Studio	2.20	build110707	All	All
Application	Iconcool	Pdfcool Studio	2.24	build1110801	All	All
Application	Iconcool	Pdfcool Studio	2.26	build110823	All	All
Application	Iconcool	Pdfcool Studio	2.30	build110920	All	All
Application	Iconcool	Pdfcool Studio	2.40	build111016	All	All
Application	Iconcool	Pdfcool Studio	2.5	build120405	All	All
Application	Iconcool	Pdfcool Studio	2.6	build120405	All	All
Application	Iconcool	Pdfcool Studio	2.7	build120405	All	All
Application	Iconcool	Pdfcool Studio	2.8	build120518	All	All
Application	Iconcool	Pdfcool Studio	3.0	build121022	All	All
Application	Iconcool	Pdfcool Studio	All	build130330	All	All
cpe:2.3:a:iconcool:pdfcool_studio:2.0:build110427:*****:						
cpe:2.3:a:iconcool:pdfcool_studio:2.0:build110502:*****:						
cpe:2.3:a:iconcool:pdfcool_studio:2.0:build110508:*****:						
cpe:2.3:a:iconcool:pdfcool_studio:2.0:build110510:*****:						
cpe:2.3:a:iconcool:pdfcool_studio:2.0:build110512:*****:						
cpe:2.3:a:iconcool:pdfcool_studio:2.10:build110519:*****:						
cpe:2.3:a:iconcool:pdfcool_studio:2.10:build110523:*****:						
cpe:2.3:a:iconcool:pdfcool_studio:2.12:build110528:*****:						
cpe:2.3:a:iconcool:pdfcool_studio:2.14:build110608:*****:						
cpe:2.3:a:iconcool:pdfcool_studio:2.16:build110612:*****:						
cpe:2.3:a:iconcool:pdfcool_studio:2.20:build110707:*****:						
cpe:2.3:a:iconcool:pdfcool_studio:2.24:build1110801:*****:						
cpe:2.3:a:iconcool:pdfcool_studio:2.26:build110823:*****:						
cpe:2.3:a:iconcool:pdfcool_studio:2.30:build110920:*****:						
cpe:2.3:a:iconcool:pdfcool_studio:2.40:build111016:*****:						
cpe:2.3:a:iconcool:pdfcool_studio:2.5:build120405:*****:						

```
cpe:2.3:a:iconcool:pdfcool_studio:2.6:build120405:*:*:*:*:*:
```

```
cpe:2.3:a:iconcool:pdfcool_studio:2.7:build120405:*:*:*:*:*:
```

```
cpe:2.3:a:iconcool:pdfcool_studio:2.8:build120518:*.x86_64:*
```

```
cpe:2.3:a:iconcool:pdfcool_studio:3.0:build121022:*:*:*:*:*
```

```
cpe:2.3:a:iconcool:pdfcool_studio:2.0:build110427:*.***.*.*.*.*
```

```
cpe:2.3:a:iconcool:pdfcool_studio:2.0:build110502:*. (*.*)
```

```
cpe:2.3:a:iconcool:pdfcool_studio:2.0:build110508:*:*:*:*.*
```

```
cpe:2.3:a:iconcool:pdfcool_studio:2.0:build110510:*.***.***.
```

```
cpe:2.3:a:iconcool:pdfcool_studio:2.0:build110512:*.***.***.
```

```
cpe:2.3:a:iconcool:pdfcool_studio:2.10:build110519:*.*.~*~*~*~*~*~*
```

```
cpe:2.3:a:iconcool:pdfcool_studio:2.10:build110523:*.?:*.?:*.?:*
```

```
cpe:2.3:a:iconcool:pdfcool_studio:2.12:build110528:*.*.~*~*~*~*~*~*
```

cpe:2.3:a:iconcool:pdfcool_studio:2.14:build110608:*:*:*:*:*

```
cpe:2.3:a:iconcool:pdfcool_studio:2.16:build110612:*:*:*:*:*
```

cpe:2.3:a:iconcool:pdfcool_studio:2.20:build110707:*:*:*:*:

```
cpe:2.3:a:iconcool:pdfcool_studio:2.24:build1110801:*.x86_64:*
```

```
cpe:2.3:a:iconcool:pdfcool_studio:2.26:build110823:*.?:*.?:*.?:*
```

```
cpe:2.3:a:iconcool:pdfcool_studio:2.30:build110920:*:*:*:*.*
```

```
cpe:2.3:a:iconcool:pdfcool_studio:2.40:build111016:*:*:*:*.*
```

```
cpe:2.3:a:iconcool:pdfcool_studio:2.5:build120405:*.?:*.?:*.?:*
```

```
cpe:2.3:a:iconcool:pdfcool_studio:2.6:build120405:*.x86_64.rpm
```

```
cpe:2.3:a:iconcool:pdfcool_studio:2.7:build120405:*.x86_64.rpm
```

```
cpe:2.3:a:iconcool:pdfcool studio:2.8:build120518:*:*:*:*:*:
```

```
cpe:2.3:a:iconcool:pdfcool_studio:3.0:build121022:*:*:*:*:*:
```

```
cpe:2.3:a:iconcool:pdfcool_studio:*:build130330:*:*:*:*:*:
```

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](#)