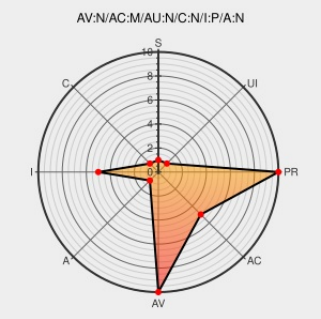
# CVE-2009-2217

Published on: 06/25/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:31 PM UTC

## CVE-2009-2217

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




Certain versions of Nbbc from Phantom-inker contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in NBBC before 1.4.2 allows remote attackers to inject arbitrary web script or HTML via an invalid URL in a BBCode img tag.

CVE-2009-2217 has been assigned by cve@mitre.org to track the vulnerability

### CVSS2 Score: 4.3 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | PARTIAL | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| NBBC "[img]" BBCode Script Insertion Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com | Vendor Advisory, web.archive.org, text/html | SECUNIA 35520 |
| IBM X-Force Exchange | exchange.xforce.ibmcloud.com, text/html | XF nbbc-img-xss(51288) |
| NBBC / Discussion / Help: Injection in [img] tags? | Patch, sourceforge.net, text/html | CONFIRM sourceforge.net/forum/message.php?msg_id=7456208 |
| No Description Provided | osvdb.org, Inactive Link, Not Archived | OSVDB 55266 |
| NBBC / Bugs / #8 Security: [img] tags emit raw text for invalid URLs | Patch, sourceforge.net | CONFIRM sourceforge.net/tracker/?func=detail&aid=2809888&group_id=235382&atid=1096820 |

| | | |
|---|---|---|
| | text/html | |
| NBBC / Discussion / Help: Injection in [img] tags? | Patch<br>sourceforge.net<br>text/html | MISC sourceforge.net/forum/message.php?msg_id=7455625 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Phantom-inker | Nbbc | 1.0 | All | All | All |
| Application | Phantom-inker | Nbbc | 1.0 | rc | All | All |
| Application | Phantom-inker | Nbbc | 1.0 | rc2 | All | All |
| Application | Phantom-inker | Nbbc | 1.0 | rc3 | All | All |
| Application | Phantom-inker | Nbbc | 1.0 | rc4 | All | All |
| Application | Phantom-inker | Nbbc | 1.0 | rc5 | All | All |
| Application | Phantom-inker | Nbbc | 1.1 | All | All | All |
| Application | Phantom-inker | Nbbc | 1.2 | All | All | All |
| Application | Phantom-inker | Nbbc | 1.3 | All | All | All |
| Application | Phantom-inker | Nbbc | 1.3.1 | All | All | All |
| Application | Phantom-inker | Nbbc | 1.3.2 | All | All | All |
| Application | Phantom-inker | Nbbc | 1.3.3 | All | All | All |
| Application | Phantom-inker | Nbbc | 1.3.4 | All | All | All |
| Application | Phantom-inker | Nbbc | 1.4.0 | All | All | All |
| Application | Phantom-inker | Nbbc | alpha | All | All | All |
| Application | Phantom-inker | Nbbc | 1.0 | All | All | All |
| Application | Phantom-inker | Nbbc | 1.0 | rc | All | All |
| Application | Phantom-inker | Nbbc | 1.0 | rc2 | All | All |
| Application | Phantom-inker | Nbbc | 1.0 | rc3 | All | All |
| Application | Phantom-inker | Nbbc | 1.0 | rc4 | All | All |
| Application | Phantom-inker | Nbbc | 1.0 | rc5 | All | All |
| Application | Phantom-inker | Nbbc | 1.1 | All | All | All |
| Application | Phantom-inker | Nbbc | 1.2 | All | All | All |
| Application | Phantom-inker | Nbbc | 1.3 | All | All | All |
| Application | Phantom-inker | Nbbc | 1.3.1 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Phantom-inker | Nbbc | 1.3.2 | All | All | All |
| Application | Phantom-inker | Nbbc | 1.3.3 | All | All | All |
| Application | Phantom-inker | Nbbc | 1.3.4 | All | All | All |
| Application | Phantom-inker | Nbbc | 1.4.0 | All | All | All |
| Application | Phantom-inker | Nbbc | alpha | All | All | All |
| Application | Phantom-inker | Nbbc | All | All | All | All |

cpe:2.3:a:phantom-inker:nbbc:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.0:rc:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.0:rc4:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.0:rc5:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.3:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:alpha:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.0:rc:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.0:rc4:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.0:rc5:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.3:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:alpha:*:*:*:*:*:*:*:

cpe:2.3:a:phantom-inker:nbbc:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→