



CVE-2002-1624

Published on: 12/31/2002 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:01 PM UTC

CVE-2002-1624

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

Certain versions of [Lotus Domino](#) from [Ibm](#) contain the following vulnerability:

Buffer overflow in Lotus Domino web server before R5.0.10, when logging to DOMLOG.NSF, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long HTTP Authenticate header containing certain non-ASCII characters.

CVE-2002-1624 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

PARTIAL

CVE References

Description

Tags

Link

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](https://exchange.xforce.ibmcloud.com/text/html)
text/html

[XF lotus-domino-authentication-bo\(11058\)](#)

CERT/CC Vulnerability Note VU#772563

[US Government Resource](#)
www.kb.cert.org
text/html

[CERT-VN VU#772563](#)

Lotus Domino HTTP Authentication Logging Buffer Overflow Vulnerability

[Patch](#)
[cve.report \(archive\)](#)
text/html

[BID 6646](#)

IBM Lotus Domino Web Server Buffer Overflow During Authentication May Let Remote Users Crash the Web Server - SecurityTracker

[securitytracker.com](https://securitytracker.com/text/html)
text/html

[SECTrack 1004052](#)

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 selecting these links, you may be leaving CVEreport's website. We have provided these links to other resources 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	ibm	Lotus Domino	5.0	All	All	All
Application	ibm	Lotus Domino	5.0.1	All	All	All
Application	ibm	Lotus Domino	5.0.2	All	All	All
Application	ibm	Lotus Domino	5.0.3	All	All	All
Application	ibm	Lotus Domino	5.0.4	All	solaris	All
Application	ibm	Lotus Domino	5.0.4a	All	All	All
Application	ibm	Lotus Domino	5.0.5	All	All	All
Application	ibm	Lotus Domino	5.0.6	All	All	All
Application	ibm	Lotus Domino	5.0.6a	All	All	All
Application	ibm	Lotus Domino	5.0.7	All	solaris	All
Application	ibm	Lotus Domino	5.0.7a	All	All	All
Application	ibm	Lotus Domino	5.0.8	All	All	All
Application	ibm	Lotus Domino	5.0.9	All	All	All
Application	ibm	Lotus Domino	5.0.9a	All	All	All
Application	ibm	Lotus Domino	5.0	All	All	All
Application	ibm	Lotus Domino	5.0.1	All	All	All
Application	ibm	Lotus Domino	5.0.2	All	All	All
Application	ibm	Lotus Domino	5.0.3	All	All	All
Application	ibm	Lotus Domino	5.0.4	All	solaris	All
Application	ibm	Lotus Domino	5.0.4a	All	All	All
Application	ibm	Lotus Domino	5.0.5	All	All	All
Application	ibm	Lotus Domino	5.0.6	All	All	All
Application	ibm	Lotus Domino	5.0.6a	All	All	All
Application	ibm	Lotus Domino	5.0.7	All	solaris	All
Application	ibm	Lotus Domino	5.0.7a	All	All	All
Application	ibm	Lotus Domino	5.0.8	All	All	All
Application	ibm	Lotus Domino	5.0.9	All	All	All
Application	ibm	Lotus Domino	5.0.9a	All	All	All

```
cpe:2.3:a:ibm:lotus_domino:5.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:5.0.1:*:*:*:*:*:
```

cpe:2.3:a:ibm:lotus_domino:5.0.2:*:*:*:*:*:*:

```
cpe:2.3:a:ibm:lotus_domino:5.0.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:5.0.4:*:solaris:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:5.0.4a:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:5.0.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:5.0.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:5.0.6a:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:5.0.7:*:solaris:*:*:*:*:
```

cpe:2.3:a:ibm:lotus_domino:5.0.7a:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:5.0.8:*:*:*:*:*:*:

```
cpe:2.3:a:ibm:lotus_domino:5.0.9:*:*:*:*:*:
```

cpe:2.3:a:ibm:lotus_domino:5.0.9a:*:*:*:*:*:*:

```
cpe:2.3:a:ibm:lotus_domino:5.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:5.0.1:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:5.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:5.0.3:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:5.0.4:*:solaris:*:*:*:*:
```

cpe:2.3:a:ibm:lotus_domino:5.0.4a:*:*:*:*:*:*:

```
cpe:2.3:a:ibm:lotus_domino:5.0.5:*:*:*:*:*:*:
```

cpe:2.3:a:ibm:lotus_domino:5.0.6:*:*:*:*:*:*:

```
cpe:2.3:a:ibm:lotus_domino:5.0.6a:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:5.0.7:*:solaris:*:*:*:*:*
```

cpe:2.3:a:ibm:lotus_domino:5.0.7a:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:5.0.8:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:5.0.9:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:5.0.9a:*.:.:.:.:.:

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](#)