

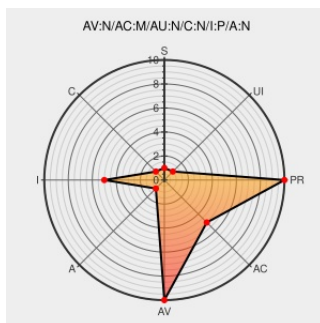


CVE-2012-3301

Published on: 08/21/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:16 PM UTC

CVE-2012-3301

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

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

Multiple CRLF injection vulnerabilities in the HTTP server in IBM Lotus Domino 8.5.x before 8.5.4 allow remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via crafted input involving (1) Mozilla Firefox 3.0.9 and earlier or (2) unspecified browsers.

CVE-2012-3301 has been assigned by psirt@us.ibm.com 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

IBM X-Force Exchange

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

[XF lotus-domino-response-splitting\(77400\)](#)

HTTPRS та XSS уразливості в IBM Lotus Domino - Websecurity - Веб безпека

[websecurity.com.ua](#)
[text/html](#)

[MISC websecurity.com.ua/5839/](#)

IBM Security Bulletin: Aug-2012 IBM Lotus Domino Web Server Cross-Site Scripting Vulnerabilities (CVE-2012-3302, CVE-2012-3301) - United States

[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

[CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21608160](#)

By selecting these links, you may be leaving CVEreport workspace. 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	ibm	Lotus Domino	8.5.0	All	All	All
Application	ibm	Lotus Domino	8.5.0.1	All	All	All
Application	ibm	Lotus Domino	8.5.1.1	All	All	All
Application	ibm	Lotus Domino	8.5.1.2	All	All	All
Application	ibm	Lotus Domino	8.5.1.3	All	All	All
Application	ibm	Lotus Domino	8.5.1.4	All	All	All
Application	ibm	Lotus Domino	8.5.1.5	All	All	All
Application	ibm	Lotus Domino	8.5.2.0	All	All	All
Application	ibm	Lotus Domino	8.5.2.1	All	All	All
Application	ibm	Lotus Domino	8.5.2.2	All	All	All
Application	ibm	Lotus Domino	8.5.2.3	All	All	All
Application	ibm	Lotus Domino	8.5.2.4	All	All	All
Application	ibm	Lotus Domino	8.5.3.0	All	All	All
Application	ibm	Lotus Domino	8.5.3.1	All	All	All
Application	ibm	Lotus Domino	8.5.3.2	All	All	All
Application	ibm	Lotus Domino	8.5.0	All	All	All
Application	ibm	Lotus Domino	8.5.0.1	All	All	All
Application	ibm	Lotus Domino	8.5.1.1	All	All	All
Application	ibm	Lotus Domino	8.5.1.2	All	All	All
Application	ibm	Lotus Domino	8.5.1.3	All	All	All
Application	ibm	Lotus Domino	8.5.1.4	All	All	All
Application	ibm	Lotus Domino	8.5.1.5	All	All	All
Application	ibm	Lotus Domino	8.5.2.0	All	All	All
Application	ibm	Lotus Domino	8.5.2.1	All	All	All
Application	ibm	Lotus Domino	8.5.2.2	All	All	All
Application	ibm	Lotus Domino	8.5.2.3	All	All	All
Application	ibm	Lotus Domino	8.5.2.4	All	All	All
Application	ibm	Lotus Domino	8.5.3.0	All	All	All
Application	ibm	Lotus Domino	8.5.3.1	All	All	All
Application	ibm	Lotus Domino	8.5.3.2	All	All	All

```
cpe:2.3:a:ibm:lotus_domino:8.5.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.0.1:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.1.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.1.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.1.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.1.4:*.:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.1.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.2.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.2.1:::*:*:*:*:
```

cpe:2.3:a:ibm:lotus_domino:8.5.2.2:*:*:*:*:*:

```
cpe:2.3:a:ibm:lotus_domino:8.5.2.3:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.2.4:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.3.0:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.3.1:::*:*:*:*:
```

cpe:2.3:a:ibm:lotus_domino:8.5.3.2:*:*:*:*:*:

```
cpe:2.3:a:ibm:lotus_domino:8.5.0:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.0.1:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.1.1:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.1.2:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.1.3:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.1.4:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.1.5:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.2.0:*.~*~*~*~*~*~*
```

cpe:2.3:a:ibm:lotus_domino:8.5.2.1:*.~*~*~*~*~*~*

```
cpe:2.3:a:ibm:lotus_domino:8.5.2.2:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.2.3:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.2.4:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:lotus_domino:8.5.3.0:*:*:*:*:*:
```

cpe:2.3:a:ibm:lotus_domino:8.5.3.1:*.~*~*~*~*~*~*

cpe:2.3:a:ibm:lotus_domino:8.5.3.2:*****:

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](#)