



CVE-2015-5040

Published on: 10/29/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:15 PM UTC

CVE-2015-5040

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

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

Buffer overflow in IBM Domino 8.5.1 through 8.5.3 before 8.5.3 FP6 IF10 and 9.x before 9.0.1 FP4 IF3 allows remote attackers to execute arbitrary code or cause a denial of service (SMTP daemon crash) via a crafted GIF image, aka SPRs KLYH9ZDKRE and KLYH9ZTLEZ, a different vulnerability than CVE-2015-4994.

CVE-2015-5040 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

IBM Lotus Domino GIF File Processing Flaw Lets Remote Users Execute Arbitrary C ode - SecurityTracker

[www.securitytracker.com](#)
[text/html](#)

[SECTrack 1033974](#)

IBM Security Bulletin: Multiple Vulnerabilities in IBM Domino GIF Processing (CVE-2015-4994, CVE-2015-5040) - United States

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

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

[CONFIRM](#) [www-01.ibm.com/support/docview.wss?uid=swg21969050](#)

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	IBM	Domino	8.5.0	All	All	All
Application	IBM	Domino	8.5.0.1	All	All	All
Application	IBM	Domino	8.5.1	All	All	All
Application	IBM	Domino	8.5.1.1	All	All	All
Application	IBM	Domino	8.5.1.2	All	All	All
Application	IBM	Domino	8.5.1.3	All	All	All
Application	IBM	Domino	8.5.1.4	All	All	All
Application	IBM	Domino	8.5.1.5	All	All	All
Application	IBM	Domino	8.5.2	All	All	All
Application	IBM	Domino	8.5.2.1	All	All	All
Application	IBM	Domino	8.5.2.2	All	All	All
Application	IBM	Domino	8.5.2.3	All	All	All
Application	IBM	Domino	8.5.2.4	All	All	All
Application	IBM	Domino	8.5.3	All	All	All
Application	IBM	Domino	8.5.3.1	All	All	All
Application	IBM	Domino	8.5.3.2	All	All	All
Application	IBM	Domino	8.5.3.3	All	All	All
Application	IBM	Domino	8.5.3.4	All	All	All
Application	IBM	Domino	8.5.3.5	All	All	All
Application	IBM	Domino	8.5.3.6	All	All	All
Application	IBM	Domino	9.0.1	All	All	All
Application	IBM	Domino	9.0.1.1	All	All	All
Application	IBM	Domino	9.0.1.2	All	All	All
Application	IBM	Domino	9.0.1.3	All	All	All
Application	IBM	Domino	9.0.1.4	All	All	All
Application	IBM	Domino	8.5.0	All	All	All
Application	IBM	Domino	8.5.0.1	All	All	All
Application	IBM	Domino	8.5.1	All	All	All
Application	IBM	Domino	8.5.1.1	All	All	All
Application	IBM	Domino	8.5.1.2	All	All	All
Application	IBM	Domino	8.5.1.3	All	All	All
Application	IBM	Domino	8.5.1.4	All	All	All

Application	ibm	Domino	8.5.1.5	All	All	All
Application	ibm	Domino	8.5.2	All	All	All
Application	ibm	Domino	8.5.2.1	All	All	All
Application	ibm	Domino	8.5.2.2	All	All	All
Application	ibm	Domino	8.5.2.3	All	All	All
Application	ibm	Domino	8.5.2.4	All	All	All
Application	ibm	Domino	8.5.3	All	All	All
Application	ibm	Domino	8.5.3.1	All	All	All
Application	ibm	Domino	8.5.3.2	All	All	All
Application	ibm	Domino	8.5.3.3	All	All	All
Application	ibm	Domino	8.5.3.4	All	All	All
Application	ibm	Domino	8.5.3.5	All	All	All
Application	ibm	Domino	8.5.3.6	All	All	All
Application	ibm	Domino	9.0.1	All	All	All
Application	ibm	Domino	9.0.1.1	All	All	All
Application	ibm	Domino	9.0.1.2	All	All	All
Application	ibm	Domino	9.0.1.3	All	All	All
Application	ibm	Domino	9.0.1.4	All	All	All
cpe:2.3:a:ibm:domino:8.5.0:*****:						
cpe:2.3:a:ibm:domino:8.5.0.1:*****:						
cpe:2.3:a:ibm:domino:8.5.1:*****:						
cpe:2.3:a:ibm:domino:8.5.1.1:*****:						
cpe:2.3:a:ibm:domino:8.5.1.2:*****:						
cpe:2.3:a:ibm:domino:8.5.1.3:*****:						
cpe:2.3:a:ibm:domino:8.5.1.4:*****:						
cpe:2.3:a:ibm:domino:8.5.1.5:*****:						
cpe:2.3:a:ibm:domino:8.5.2:*****:						
cpe:2.3:a:ibm:domino:8.5.2.1:*****:						
cpe:2.3:a:ibm:domino:8.5.2.2:*****:						
cpe:2.3:a:ibm:domino:8.5.2.3:*****:						
cpe:2.3:a:ibm:domino:8.5.2.4:*****:						
cpe:2.3:a:ibm:domino:8.5.3:*****:						

cpe:2.3:a:ibm:domino:8.5.3.1:*****:
cpe:2.3:a:ibm:domino:8.5.3.2:*****:
cpe:2.3:a:ibm:domino:8.5.3.3:*****:
cpe:2.3:a:ibm:domino:8.5.3.4:*****:
cpe:2.3:a:ibm:domino:8.5.3.5:*****:
cpe:2.3:a:ibm:domino:8.5.3.6:*****:
cpe:2.3:a:ibm:domino:9.0.1:*****:
cpe:2.3:a:ibm:domino:9.0.1.1:*****:
cpe:2.3:a:ibm:domino:9.0.1.2:*****:
cpe:2.3:a:ibm:domino:9.0.1.3:*****:
cpe:2.3:a:ibm:domino:9.0.1.4:*****:
cpe:2.3:a:ibm:domino:8.5.0:*****:
cpe:2.3:a:ibm:domino:8.5.0.1:*****:
cpe:2.3:a:ibm:domino:8.5.1:*****:
cpe:2.3:a:ibm:domino:8.5.1.1:*****:
cpe:2.3:a:ibm:domino:8.5.1.2:*****:
cpe:2.3:a:ibm:domino:8.5.1.3:*****:
cpe:2.3:a:ibm:domino:8.5.1.4:*****:
cpe:2.3:a:ibm:domino:8.5.1.5:*****:
cpe:2.3:a:ibm:domino:8.5.2:*****:
cpe:2.3:a:ibm:domino:8.5.2.1:*****:
cpe:2.3:a:ibm:domino:8.5.2.2:*****:
cpe:2.3:a:ibm:domino:8.5.2.3:*****:
cpe:2.3:a:ibm:domino:8.5.2.4:*****:
cpe:2.3:a:ibm:domino:8.5.3:*****:
cpe:2.3:a:ibm:domino:8.5.3.1:*****:
cpe:2.3:a:ibm:domino:8.5.3.2:*****:
cpe:2.3:a:ibm:domino:8.5.3.3:*****:

cpe:2.3:a:ibm:domino:8.5.3.4:*****:
cpe:2.3:a:ibm:domino:8.5.3.5:*****:
cpe:2.3:a:ibm:domino:8.5.3.6:*****:
cpe:2.3:a:ibm:domino:9.0.1:*****:
cpe:2.3:a:ibm:domino:9.0.1.1:*****:
cpe:2.3:a:ibm:domino:9.0.1.2:*****:
cpe:2.3:a:ibm:domino:9.0.1.3:*****:
cpe:2.3:a:ibm:domino:9.0.1.4:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →