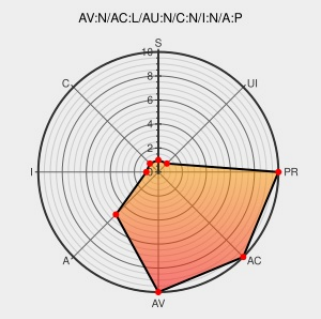
CVE-2005-1441

Published on: 05/03/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1441

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



Certain versions of Lotus Domino from Ibm contain the following vulnerability:

Format string vulnerability in Lotus Domino 6.0.x before 6.0.5 and 6.5.x before 6.5.4 allows remote attackers to cause a denial of service via the Notes protocol (NRPC).

CVE-2005-1441 has been assigned by 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, text/html	XF lotus-nrpc-format-string(20043)
Lotus Domino Format String Flaw in Processing NRPC Protocol Lets Remote Users Deny Service - SecurityTracker	securitytracker.com, text/html	SECTRACK 1013842
Secunia - Advisories - Lotus Notes/Domino Multiple Vulnerabilities	web.archive.org, text/html	SECUNIA 14879
IBM Lotus Domino Server Notes Remote Procedure Call Remote Format String Vulnerability	cve.report (archive), text/html	BID 13446
IBM Potential Denial of Service Vulnerability During Notes Authentication - United States	Patch, web.archive.org, text/html, Inactive Link, Not Archived	CONFIRM www-1.ibm.com/support/docview.wss?rs=463&uid=swg21202525

No Description Provided

www.osvdb.org

OSVDB 15366

Inactive Link Not Archived

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	Lotus Domino	6.0	All	All	All
Application	Ibm	Lotus Domino	6.0.1	All	All	All
Application	Ibm	Lotus Domino	6.0.2	All	All	All
Application	Ibm	Lotus Domino	6.0.2_cf2	All	All	All
Application	Ibm	Lotus Domino	6.0.3	All	All	All
Application	Ibm	Lotus Domino	6.5.0	All	All	All
Application	Ibm	Lotus Domino	6.5.1	All	All	All
Application	Ibm	Lotus Domino	6.5.2	All	All	All
Application	Ibm	Lotus Domino	6.5.3	All	All	All
Application	Ibm	Lotus Domino	6.0	All	All	All
Application	Ibm	Lotus Domino	6.0.1	All	All	All
Application	Ibm	Lotus Domino	6.0.2	All	All	All
Application	Ibm	Lotus Domino	6.0.2_cf2	All	All	All
Application	Ibm	Lotus Domino	6.0.3	All	All	All
Application	Ibm	Lotus Domino	6.5.0	All	All	All
Application	Ibm	Lotus Domino	6.5.1	All	All	All
Application	Ibm	Lotus Domino	6.5.2	All	All	All
Application	Ibm	Lotus Domino	6.5.3	All	All	All

cpe:2.3:a:ibm:lotus_domino:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:6.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:6.0.2_cf2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:6.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:6.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:6.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:6.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:6.5.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:6.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:6.0.2_cf2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:6.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:6.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:6.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:6.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_domino:6.5.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→