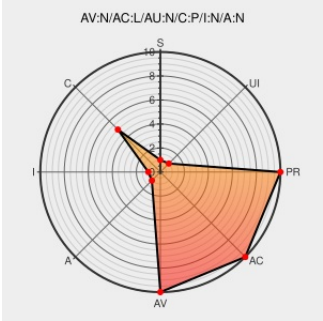
CVE-2005-2428

Published on: 08/03/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2428

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



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

Lotus Domino R5 and R6 WebMail, with "Generate HTML for all fields" enabled, stores sensitive data from names.nsf in hidden form fields, which allows remote attackers to read the HTML source to obtain sensitive information such as (1) the password hash in the HTTPPassword field, (2) the password change date in the HTTPPasswordChangeDate field, (3) the client platform in the ClntPltfrm field, (4) the client machine name in the ClntMachine field, and (5) the client Lotus Domino release in the ClntBld field, a different vulnerability than CVE-2005-2696.

CVE-2005-2428 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**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF lotus-domino-names-obtain-information(21556)
Secunia - Advisories - Lotus Domino Webmail Information Disclosure Security Issue	Vendor Advisory web.archive.org text/html	SECUNIA 16231
'CYBSEC - Security Advisory: Default	marc.info text/html	BUGTRAQ 20050726 CYBSEC - Security Advisory: Default Configuration Information

Advisory: Default Configuration Information' - MARC	text/html	Information
IBM Lotus Domino Password Encryption Weakness	cve.report (archive) text/html	BID 14389
	Vendor Advisory www.cybsec.com application/pdf	MISC www.cybsec.com/vuln/default_configuration_information_disclosure_lotus_domino.pd
SecurityTracker.com Archives - IBM Lotus Domino Discloses Hashed Passwords and Other Information to Remote Authenticated Users	securitytracker.com text/html	SECTRACK 1014584
IBM Lotus Domino R8 - Password Hash Extraction - Windows webapps Exploit	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 39495
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 18462
SecuriTeam.com ™ - Default Configuration Information Disclosure in Lotus Domino (Including Password Hashes)	www.securiteam.com text/html	MISC www.securiteam.com/securitynews/5FP0E15GLQ.html
IBM notice: The page you requested cannot be displayed	Vendor Advisory www-1.ibm.com text/html Inactive Link Not Archived	CONFIRM www-1.ibm.com/support/docview.wss?uid=swg21212934

There are currently no QIDs associated with this CVE

Exploit/POC from Github

IBM Lotus Domino <= R8 Password Hash Extraction Exploit

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	6.0	All	All	All
Application	Ibm	Lotus Domino	6.5	All	All	All

Application	Ibm	Lotus Domino	5.0	All	All	All
Application	Ibm	Lotus Domino	6.0	All	All	All
Application	Ibm	Lotus Domino	6.5	All	All	All

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

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

cpe:2.3:a:ibm:lotus_domino:6.5:*:*:*:*:*:*:*:

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

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

cpe:2.3:a:ibm:lotus_domino:6.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→