

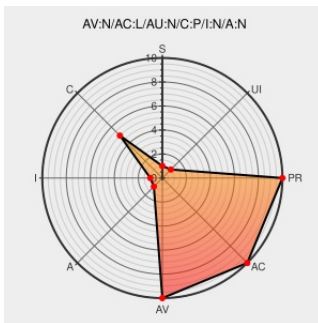


# CVE-2005-2428

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 [M](#) [cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access  
Vector

**NETWORK**

Access  
Complexity

**LOW**

Authentication

**NONE**

Confidentiality  
Impact

**PARTIAL**

Integrity  
Impact

**NONE**

Availability  
Impact

**NONE**

## CVE References

Description

Tags

Link

IBM X-Force  
Exchange

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

[lotus-domino-names-obtain-information\(21556\)](#)

Secunia - Advisories -  
Lotus Domino  
Webmail Information  
Disclosure Security  
Issue

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

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](mailto:comment@cve.report).

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                               | <a href="#">ibm</a> | <a href="#">Lotus Domino</a> | 5.0 | All | All | All |
| Application                               | <a href="#">ibm</a> | <a href="#">Lotus Domino</a> | 6.0 | All | All | All |
| Application                               | <a href="#">ibm</a> | <a href="#">Lotus Domino</a> | 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 →](#)