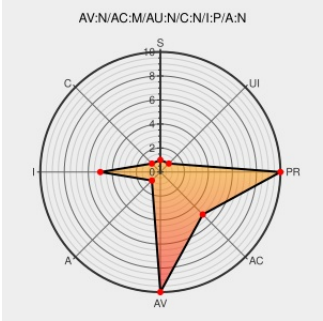
# CVE-2004-1621

Published on: 10/18/2004 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

## CVE-2004-1621

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




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

** DISPUTED ** NOTE: this issue has been disputed by the vendor. Cross-site scripting (XSS) vulnerability in IBM Lotus Notes R6 and Domino R6, and possibly earlier versions, allows remote attackers to execute arbitrary web script or HTML via square brackets at the beginning and end of (1) computed for display, (2) computed when composed, or (3) computed text element fields. NOTE: the vendor has disputed this issue, saying that it is not a problem with Notes/Domino itself, but with the applications that do not properly handle this feature.

CVE-2004-1621 has been assigned by cve@mitre.org 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 |
|---|---|---|
| CERT Vulnerability Notes Database | US Government Resource, www.kb.cert.org, text/html, Inactive Link, Not Archived | CERT-VN VU#404382 |
| Secunia - Advisories - IBM Lotus Domino Server Potential Cross-Site Scripting Security Issue | Exploit, Vendor Advisory, web.archive.org, text/html | SECUNIA 12891 |
| IBM notice: The page you requested cannot be displayed | Exploit | MISC www |

| | | |
|---|---|---|
| IBM notice: The page you requested cannot be displayed | Exploit<br>Vendor Advisory<br>www-1.ibm.com<br>text/html<br>Inactive Link Not Archived | MISC www-1.ibm.com/support/docview.wss?rs=463&uid=swg21187833 |
| IBM X-Force Exchange | exchange.xforce.ibmcloud.com<br>text/html | XF lotus-notes-xss(17758) |
| SecurityTracker.com Archives - Lotus Notes/Domino Square Bracket Encoding Failure Lets Remote Users Conduct Cross-Site Scripting Attacks | Exploit<br>Vendor Advisory<br>securitytracker.com<br>text/html | SECTRACK 1011779 |
| 'IBM Lotus Notes/Domino fails to encode Square Brackets ( [ ] )' - MARC | marc.info<br>text/html | BUGTRAQ 20041018 IBM Lotus Notes/Domino fails to encode Square Brackets ( [ ] ) |
| IBM Lotus Domino Cross-Site Scripting and HTML Injection Vulnerabilities | Exploit<br>Vendor Advisory<br>cve.report (archive)<br>text/html | BID 11458 |
| 'Re: IBM Lotus Notes/Domino fails to encode Square Brackets ( [ ]' - MARC | marc.info<br>text/html | BUGTRAQ 20041021 Re: IBM Lotus Notes/Domino fails to encode Square Brackets ( [ ] ) |



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 | 6.0 | 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 |

- 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:6.0:*:*:*:*:*:*:*:
- 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:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→