

[NEWS] Lotus Notes/Domino Web Retriever HTTP Status Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-03/0031.html>

From: support@securiteam.com

Date: 03/16/03

From: support@securiteam.com

To: list@securiteam.com

Date: 16 Mar 2003 12:34:03 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Lotus Notes/Domino Web Retriever HTTP Status Buffer Overflow

SUMMARY

The Lotus Notes/Domino Web Retriever task is responsible for retrieving web pages on behalf of Notes users who want to access the web via their Notes server.

The Web Retriever program will crash when it receives an overly long HTTP status line from a remote web server.

If the Web Retriever is running as a server task, the crash will cause a denial of service on the server. If the Web Retriever is running locally on a client, the crash will bring down the Notes client with it.

DETAILS

Vulnerable systems:

- * Lotus Notes/Domino R4.5 server and client
- * Lotus Notes/Domino R4.6 server and client
- * Lotus Notes/Domino R5 server and client

Securiteam: [NEWS] Lotus Notes/Domino Web Retriever HTTP Status Buffer Overflow

* Lotus Notes/Domino R6 beta (pre-Gold) server and client

Immune systems:

- * Lotus Notes/Domino R6.0 Gold
- * Lotus Notes/Domino R6.0.1
- * Lotus Notes/Domino R5.0.12

By issuing an overly long status message in its HTTP response, a remote server can crash the Web Retriever process. The response line consists of the standard HTTP version and code followed by an overly long (~6000 bytes) status message, followed by two carriage return/linefeed pairs.

```
HTTP/1.1 200 Ax6000
```

A response length of around 6000 bytes is usually sufficient to crash the Web Retriever. Using a somewhat smaller buffer will still corrupt the heap, but the crash may not occur until the corrupted portions of the heap are later used.

Vendor status and information:

Lotus was notified and they have fixed this vulnerability. Lotus is tracking this issue with SPR #KSPR5DFJTR. [1] IBM has also prepared Technote #1105060, which discusses this vulnerability. [2] See the References section for more information.

Solution:

Users running R5 should upgrade to Notes R5.0.12. Users of R6 pre-Gold releases should upgrade R6.0 Gold or higher. Due to other vulnerabilities discovered in R6.0 Gold, you should consider upgrading to R6.0.1, which was released in February 2003.

Domino incremental installers may be downloaded from the following URL:

<http://www14.software.ibm.com/webapp/download/search.jsp?go=y&rs=ESD-DMNTRSRVRi&sb=r>
<http://www14.software.ibm.com/webapp/download/search.jsp?go=y&rs=ESD-DMNTRSRVRi&sb=r>

As a workaround, you can disable the Web Retriever task on the server. To do this, first remove the 'Web' entry from the ServerTasks line in the server's NOTES.INI file, then issue the 'tell web quit' command at the server console.

In addition, consider removing the Web Retrieval database (typically /WEB.NSF) or lock down its ACL so that no users can access it. If the Web Retriever is disabled, users probably do not need access to this database.

Notes clients will be vulnerable to this if they are configured to use the Notes web browser instead of an external browser program. This option can be viewed in the Internet browser section of the current Location document.

ADDITIONAL INFORMATION

Securiteam: [NEWS] Lotus Notes/Domino Web Retriever HTTP Status Buffer Overflow

References:

[1] Lotus SPR #KSPR5DFJTR:

<<http://www-10.lotus.com/ldd/r5fixlist.nsf/Search?SearchView&Query=KSPR5DFJTR>>
<http://www-10.lotus.com/ldd/r5fixlist.nsf/Search?SearchView&Query=KSPR5DFJTR>

[2] IBM Technote #1105060:

<<http://www-1.ibm.com/support/docview.wss?rs=482&q=Domino&uid=swg21105060>>
<http://www-1.ibm.com/support/docview.wss?rs=482&q=Domino&uid=swg21105060>

The information has been provided by <<mailto:advisory@rapid7.com>> Rapid7 Security Advisories.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.