

**MWR InfoSecurity Security  
Advisory**

**IBM Lotus Domino "If-  
Modified-Since" Stack  
Overflow**

**15th October 2007**

## Contents

1	Detailed Vulnerability Description .....	5
1.1	Introduction .....	5
1.2	Technical Background.....	5
1.3	Vulnerability Details.....	5
1.4	Exploit Information.....	5
1.5	Dependencies .....	6
2	Recommendations.....	7

## IBM Lotus Domino “If-Modified-Since” Stack Overflow

Package Name:	IBM Lotus Domino Web Server
Date:	2007-10-15
Affected Versions:	The vulnerability was introduced in Lotus Domino 6.0 and all versions up to and including the following are affected: - Lotus Domino 6.5.5 FixPack 2 Lotus Domino 7.0.2 FixPack 1

CVE Reference	CVE-2007-0067 (This CVE reference does not currently provide detailed information about the nature and impact of this issue)
Author	M. Ruks
Date	15th October 2007
Severity	High
Local/Remote	Remote
Vulnerability Class	Stack Based Overflow
Vendor URL	<a href="http://www.ibm.com">www.ibm.com</a>
Version	
Vendor Response	The vendor was contacted and confirmed that the issue was addressed as part of a previous Quality Engineering case recorded as SPR# NKEN6X3NKK. However, the previously released information records this as a Denial of Service issue rather than a remote stack overflow. Nevertheless, IBM have provided software packages which resolve the issue and a link to these is included within this document.
Exploit Details Included	Yes although no exploit code is included.
Affected OS	The vulnerability has been confirmed on the Microsoft® Windows OS, however, all platforms are expected to be affected.

### Overview:

The IBM Lotus Domino Web Server service is vulnerable to a stack based buffer overflow which can be exploited remotely. Upon reporting this issue to IBM it was discovered that this was a known issue which had been resolved in a number of previous releases and Fix Packs. However, the previously reported issue did not correctly assess the impact of the vulnerability or provide a description that allowed the vulnerability of a given system to be accurately assessed.

### Impact:

The vulnerability would enable an attacker to execute arbitrary code on a system. In the majority of installations this would be with local SYSTEM privileges.

### Cause:

The code responsible for parsing a parameter within the HTTP header of requests to the service does not adequately check user supplied input. This results in the ability to overflow a stack buffer which in turn allows arbitrary code to be executed.

**Interim Workaround:**

Introduce host based or network filtering controls to restrict access to the affected service to authorised IP addresses only.

**Solution:**

This issue require the affected software to be upgraded to a secure version. The following versions are not affected by this issue: -

Lotus Domino 6.5.5 Fix Pack 3  
Lotus Domino 6.5.6  
Lotus Domino 7.0.2 Fix Pack 2  
Lotus Domino 7.0.3  
Lotus Domino 8

MWR InfoSecurity have tested a number of these versions and can confirm that they are not affected by the vulnerability as discovered. Further research effort will be devoted to confirming that the issues are correctly resolved and cannot be exploited through any other methods.

Further information about the issues can be discovered at the location given below. However, it should be noted that the description and CVSS score on the following web page do not fully reflect the information presented in this document.

<http://www-1.ibm.com/support/docview.wss?rs=477&uid=swg21257251>

## 1 Detailed Vulnerability Description

### 1.1 Introduction

The Lotus Domino Web Server is currently developed by IBM and is described by the vendor as follows: -

“IBM® Lotus® Domino® software provides world-class collaboration capabilities that can be deployed as a core e-mail and enterprise scheduling infrastructure, as a business application platform, or both.

Lotus Domino software and its client software options deliver a reliable, security-rich messaging and collaboration environment that helps companies enhance the productivity of people, streamline business processes and improve overall business responsiveness.”

Source: <http://www-142.ibm.com/software/sw-lotus/products/product4.nsf/wdocs/dominooverview>

### 1.2 Technical Background

The product can allow users to gain web based access to email and other Notes Databases. These can be designed to facilitate interaction with a wide range of business processes and applications. Notes Databases can be accessed using the HTTP protocol through the Lotus Domino web server in a similar manner to any other web enabled technology.

Domino web servers support the “If-Modified-Since” HTTP header which is a part of the protocol that is used to determine whether a page has been updated since the last time a browser accessed it. A user’s browser will request a page with this header set to the time it last received a response for the request. If the page requested had not been updated since the time presented a “304 Not Modified” response should be returned.

If the page exists and has been updated since the time presented the content will be returned in a “200 OK” response. The HTTP header of the response will contain a “Last-Modified” header with the date of the last modification of the page. The exact operation of these aspects will be specific to the implementation of the HTTP server.

### 1.3 Vulnerability Details

A vulnerability was identified in the code responsible for handling the HTTP header information provided by a user’s browser. The “If-Modified-Since” field was discovered to be taken from the HTTP header in the request and processed by the web server. The date is concatenated with the string “Last-Modified:” using a “strcat” operation with the result stored in a static sized stack buffer. Therefore, by sending an appropriate payload it is possible to overflow the stack buffer and overwrite data on the stack. This enables remote code execution to occur.

### 1.4 Exploit Information

The vulnerability can be trivially exploited by a remote attacker using an HTTP 1.1 request containing the GET method, a valid Host header and a suitably crafted If-Modified-Since header.

It is important to avoid the character 0x0a in the shellcode as this will be interpreted as a new line in the HTTP header. It is also necessary to supply a valid date in the format described within RFC 2616. The payload can then be appended to this header using the string “---” at the end of the date string. The padding to overflow the buffer, return address and shellcode could then be included after these characters.

The existence of this vulnerability has been confirmed by MWR InfoSecurity and working exploit code for the Microsoft Windows platform exists although this will not be released into the public domain at the present time. The decision to release such code in the future will be taken based on MWR InfoSecurity’s obligations to protect its customers and Critical National Infrastructure (CNI) whilst also enabling the security community to accurately assess the vulnerability of systems running the software.

## 1.5 Dependencies

To exploit this vulnerability it must be possible to make a GET request to the web server. Therefore, network filtering can be put in place to protect a server in sensitive environments. However, it is accepted that as web servers are designed to be publicly accessible this mitigation will not be possible in the majority of circumstances.

## 2 Recommendations

It is recommended that all installations of the software be upgraded to a secure version. The following versions are not affected by this issue: -

Lotus Domino 6.5.5 Fix Pack 3  
Lotus Domino 6.5.6  
Lotus Domino 7.0.2 Fix Pack 2  
Lotus Domino 7.0.3  
Lotus Domino 8

MWR InfoSecurity have tested a number of these versions and can confirm that they are not affected by the vulnerability as discovered. Further research effort will be devoted to confirming that the issues are correctly resolved and cannot be exploited through any other methods.

To reduce the level of risk to which users of the software are exposed it is advised that the application be run under a user account with the lowest level of privilege possible. It is also recommended that, where possible, Lotus Domino systems be subject to network level filtering such that only trusted IP addresses can communicate with the service. It should be noted that this is a generic recommendation and is not specific to this technology.

MWR InfoSecurity  
St. Clement House  
1-3 Alencon Link  
Basingstoke, RG21 7SB  
Tel: +44 (0)1256 300920  
Fax: +44 (0)1256 844083  
[mwrinfosecurity.com](http://mwrinfosecurity.com)