

MWR InfoSecurity Security
Advisory

IBM Lotus Domino "Accept-
Language" Stack Overflow

20th May 2008

MWR  INFOSECURITY



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 “Accept-Language” Stack Overflow

Package Name:	IBM Lotus Domino Web Server
Date:	20 th May 2008.
Affected Versions:	The vulnerability has only been confirmed in version 7.0.3 and 8.0. However, it is expected that other earlier versions will also be affected. Please refer to the vendor advisory for precise details of affected versions.

CVE Reference	CVE-2008-2240
Author	M. Ruks
Date	20 th May 2008
Severity	High
Local/Remote	Remote
Vulnerability Class	Stack Based Overflow
Vendor URL	www.ibm.com
Vendor Response	MWR InfoSecurity have been in regular contact with the vendor throughout the process of resolving the issue. Details about the IBM security fixes can be discovered at the following location: - http://www.ibm.com/support/docview.wss?rs=463&uid=swg21303057
Exploit Details Included	Limited details are included

Overview:

The IBM Lotus Domino Web Server service is vulnerable to a stack based buffer overflow which can be exploited remotely.

Impact:

The vulnerability would enable an attacker to execute arbitrary code on the system in the majority of installations this will 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 although this might not be appropriate when legitimate access to the HTTP service is required.

Solution:

Users should upgrade to the latest secure version of the product by applying the appropriate vendor provided security fix. The versions not affected by this issue are Lotus Domino 7.0.3 FixPack 1 (FP1) and 8.0.1. Information about the location of updated packages can be discovered at the following location: -

<http://www.ibm.com/support/docview.wss?rs=463&uid=swg21303057>

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 “Accept-Language” HTTP header which is a part of the protocol that is used to determine a user’s language preferences. A user’s browser will request a page with this header set to the language preference for the page they wish to receive. The server will then select the language in which to serve the page to the user.

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 “Accept Language” field was discovered to be taken from the HTTP header in the request and processed by the web server. This data is then copied to a fixed length stack buffer using the ‘strcpy’ function. Therefore, by sending an appropriate payload it is possible to overflow a stack buffer and overwrite data on the stack allowing remote code execution to occur. It should be noted that to access the code path containing the vulnerable function specially crafted characters must be included within the URL being requested..

1.4 Exploit Information

The vulnerability can be exploited by a remote attacker using an HTTP 1.1 request containing the GET method, a URL containing specific parameters, a valid Host header and a suitably crafted “Accept-Language” header. A total of 118 bytes are required after the data passed in the affected HTTP header to completely overwrite the return address of the affected function. The stack frame that must be overwritten to reach the return address contains pointers and other data that is used in other operations before the function returns. Therefore, if the



method of exploitation employed is to involve directly overwriting the return address appropriate data must be delivered in the payload to allow the function to return correctly.

.

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 should also be noted that the lack of protection mechanisms such as stack canaries makes the exploitation of these types of issue easier than when those mechanisms are in use.

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

Users should upgrade the latest secure version of the product by applying the vendor's security fixes. The versions not affected by this issue are Lotus Domino 7.0.3 FixPack 1 (FP1) and 8.0.1. Information about the location of updated packages can be discovered at the following location: -

<http://www.ibm.com/support/docview.wss?rs=463&uid=swg21303057>

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 (this is obviously not possible when running a public facing web server). It should be noted that these are generic recommendation and are 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