

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

3/2/2010

SUBJECT:

Vulnerability in IBM Lotus Domino Web Access ActiveX Control Could Allow Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in IBM Lotus Domino Web Access ActiveX control that could allow an attacker to take complete control of an affected system. ActiveX controls are small programs or animations that are embedded in Web pages which will typically enhance functionality and user experience. Domino Web Access, also known as Lotus iNotes, is a browser-based web client for Lotus Domino. IBM Lotus Domino is a server product designed for collaborative working environments such as email, scheduling, and instant messaging. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will result in a denial-of-service condition.

SYSTEMS AFFECTED:

- Domino Web Access 6.0
- Domino Web Access 6.5
- Domino Web Access 7.0 prior to 7.0.4
- Domino Web Access 8.0 prior to 8.0.2

RISK:

Government:

Large and medium government entities: **High**

Small government entities: **High**

Businesses:

Large and medium business entities: **High**

Small business entities: **High**

Home users: N/A

DESCRIPTION:

A vulnerability has been discovered in the IBM Lotus Domino Web Access ActiveX control that could allow an attacker to execute arbitrary code on an affected system. ActiveX controls are small programs or animations that are embedded in Web pages which will typically enhance

functionality and user experience. This is a buffer-overflow vulnerability which is caused by the applications' failure to perform a bounds-check on user-supplied data before copying it into an insufficiently sized buffer. This vulnerability can be exploited if a user visits a specially crafted web page designed to exploit this vulnerability. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will result in a denial-of-service condition.

The vulnerable ActiveX controls can be disabled in Internet Explorer by setting the kill bit for the following Class Identifiers (CLSIDs):

```
{3BFFE033-BF43-11d5-A271-00A024A51325}  
{983A9C21-8207-4B58-BBB8-0EBC3D7C5505}  
{E008A543-CEFB-4559-912F-C27C2B89F13B}  
{75AA409D-05F9-4f27-BD53-C7339D4B1D0A}
```

Further instructions on how to set the kill bit can be found at the following location (<http://support.microsoft.com/kb/240797>).

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade to a non-affected version of the software. This vulnerability has been mitigated in Domino Web Access 7.0.4 and 8.5. After the updated software has been installed, it is recommended that users re-visit the updated server to automatically install the non-vulnerable ActiveX control.
- Set the kill bit on the aforementioned Class Identifiers (CLSID).
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Ensure that all Microsoft Internet Explorer clients are configured to prompt before executing Active Scripting. If Active Scripting is not required it should be disabled completely.

REFERENCES:

Security Focus:

<http://www.securityfocus.com/bid/38457>

IBM:

<http://www-01.ibm.com/support/docview.wss?uid=swg21421808>

<http://www-01.ibm.com/support/docview.wss?uid=swg27018109>