

State of Alaska
State Security Office



Cyber Security Advisory

October 24, 2007

The following cyber advisory was issued by the State of Alaska and was 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.

STATE OF ALASKA ADVISORY NUMBER:

2007-023

DATE ISSUED:

October 24, 2007

SUBJECT:

IBM Lotus Notes Attachment Viewer Multiple Buffer Overflow Vulnerabilities

OVERVIEW:

A new vulnerability has been discovered in the IBM Lotus Notes email application. The vulnerability can be exploited if a user opens an email and views a malicious attachment. Successful exploitation would result in the attacker gaining the same rights as the logged-on user. This may allow the attacker to gain complete control of the system.

SYSTEMS AFFECTED:

- IBM Lotus Notes 7.0.2
- Verity Keyview Export SDK 7
- Verity Keyview Export SDK 8
- Verity Keyview Export SDK 9
- Verity Keyview Filter SDK 7
- Verity Keyview Filter SDK 8
- Verity Keyview Filter SDK 9
- Verity Keyview Viewer SDK 7
- Verity Keyview Viewer SDK 8
- Verity Keyview Viewer SDK 9

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:

Lotus Notes is a client-server, collaborative application used for accessing business e-mail, calendars and applications on an IBM Lotus Domino server. This vulnerability resides on the client side which is commonly used by the end user.

A new vulnerability has been discovered in IBM Lotus Notes that is publicly available on the Internet. The vulnerability is in the IBM Lotus Notes File Attachment Viewer, which is the default viewer for attachments in Lotus Notes. This vulnerability can be exploited if a user opens an email and views a malicious attachment. If successfully exploited, the attacker will have the same rights as the logged-on user. This may allow the attacker to execute arbitrary machine code on the affected system, which could allow for complete control of the system.

A maliciously crafted email attachment using one of the following file types can trigger this vulnerability:

- Microsoft Word (.doc)

- Dynamic Link Library (.dll)
- Microsoft Rich Text Format (.rtf)
- Portable Executable (.exe)
- Wordperfect (.wpd)
- Ami Pro (.sam)
- Adobe Acrobat FrameMaker Interchange (.mif)
- Applix Words (.aw)
- Applix Presents (.ag)

RECOMMENDATIONS:

We recommend the following actions be taken:

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not open email attachments from untrusted sources.
- Upgrade to either Lotus Notes releases 7.0.3 or 8.0, neither of which are affected by this vulnerability.
- If upgrading is not possible at this time, consider deleting the keyview.ini file in the Notes program directory. This disables ALL viewers. When a user clicks View, for any file, a dialog box will display with the message "Unable to locate the viewer configuration file." The user would then need to download or save the attachment and open the attachment with the appropriate software.

REFERENCES:

Security Focus:

<http://www.securityfocus.com/bid/26175>

IBM

<http://www-1.ibm.com/support/docview.wss?rs=899&uid=swg21271111>

<http://www-1.ibm.com/support/docview.wss?uid=swg21272836>

Vuln.sg

<http://vuln.sg/lotusnotes702-en.html>

<http://vuln.sg/lotusnotes702sam-en.html>

<http://vuln.sg/lotusnotes702doc-en.html>

<http://vuln.sg/lotusnotes702wpd-en.html>