



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

January 16, 2008

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:

2008-002

DATE ISSUED:

January 16, 2008

SUBJECT: Microsoft Excel Vulnerability

OVERVIEW:

A new vulnerability has been discovered in certain versions Microsoft Office Excel, software that processes spreadsheets. Successful exploitation will result in an attacker gaining the same user privileges as the logged on user. If the user is logged in with administrator privileges, the attacker could then install programs, view, change, or delete data, or create new accounts with full privileges. This vulnerability can be exploited by opening a malicious Excel spreadsheet (.XLS) which was emailed as an attachment, or by visiting a Web site that is hosting a malicious Excel spreadsheet.

At this time, Microsoft has confirmed this vulnerability is being used for specific targeted attacks although more widespread exploitation may occur when additional details regarding this vulnerability become available. Microsoft has not yet provided a patch.

SYSTEMS AFFECTED:

- Microsoft Office Excel 2003 Service Pack 2
- Microsoft Office Excel Viewer 2003
- Microsoft Office Excel 2002
- Microsoft Office Excel 2000
- Microsoft Office Excel 2002 Service Pack 2
- Microsoft Office Excel 2004 for Mac

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: Medium/High

DESCRIPTION:

A new vulnerability has been identified in versions of Microsoft Excel prior to Microsoft Office 2003 Service Pack 3 that may allow remote code execution. This vulnerability can be exploited by opening a malicious Excel spreadsheet (.XLS) email attachment, or by visiting a Web site that is hosting a malicious Excel spreadsheet. Successful exploitation will result in an attacker gaining the same user privileges as the logged on user. If the user is logged in with administrator privileges, the attacker could then install programs, view, change, or delete data, or create new accounts with full privileges.

There have been confirmed specific targeted attacks attempting to exploit this vulnerability. Microsoft is still investigating this vulnerability.

RECOMMENDATIONS:

We recommend the following action be taken:

- Upgrade to an unaffected software version such as Microsoft Office 2003 Service Pack 3, Office 2007 or Microsoft 2008 for Mac, after appropriate testing.
- If believe you have been affected by targeted attacks exploiting this vulnerability, please contact us immediately.

If upgrading to an unaffected version is not a viable option, we recommend that the following actions be considered:

- If you do not have a business need to receive emailed Excel spreadsheets, consider blocking them temporarily at the perimeter.
- If you do have a business need to receive emailed Excel spreadsheets, consider quarantining them and establish a process for mitigating the risk.
- Installing Microsoft Office Isolated Conversion Environment (MOICE) will protect systems running Microsoft Office 2003
- Do not visit unknown or un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments from un-trusted sources.
- Ensure that all anti-virus software is up to date with the latest signatures.
- Block un-trusted incoming traffic from the Internet at your network perimeter.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/advisory/947563.msp>

AusCERT:

<http://www.auscert.org.au/render.html?it=8654>

Washington Post:

http://blog.washingtonpost.com/securityfix/2008/01/targeted_attacks_using_unpatch.html?nav=rs_s_blog

Secunia:

<http://secunia.com/advisories/28506/>