



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

January 9, 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:

2007-02

DATE ISSUED:

01/09/2007 (original vulnerability announced early 2006)

SUBJECT:

Vulnerability in Microsoft Outlook and Microsoft Exchange Could Allow Remote Control of System

ORIGINAL OVERVIEW:

A new vulnerability has been identified in both the Microsoft Outlook Email Client and the Microsoft Exchange Email Server. Microsoft has assigned this vulnerability a severity rating of Critical due to the fact that this may allow a remote attacker to take complete control of an affected system without any user interaction. In order to exploit this vulnerability, an attacker must craft a malicious email message and send it to a vulnerable system.

No user action is required for the successful exploitation of an affected Microsoft Exchange Server; the server must only accept a specially-crafted email message. For desktops running Microsoft Outlook, successful exploitation only requires a user to open or preview the specially-crafted email message. It does not require the user to open an attachment.

Exploit code is not publicly available at the time, and Microsoft has not seen any examples of proof of concept code for either vulnerability at this time.

JAUNUARY 9 UPDATED INFORMATION:

Microsoft has released a new security bulletin (MS07-003), which is a replacement for security bulletin MS06-003. This advisory contains patches which addresses vulnerabilities in Microsoft Outlook that could allow a remote attacker to take control of an affected system.

SYSTEMS AFFECTED:

- Microsoft Office 2003 Service Pack 1, Service Pack 2
- Microsoft Office 2000 Service Pack 3 - UPDATED
- Microsoft Outlook 2000 Multilanguage Packs
- Microsoft Outlook 2000 English Multilanguage Packs

- Microsoft Outlook 2000
- Microsoft Office XP Service Pack 3 - UPDATED
- Microsoft Outlook 2002
- Microsoft Outlook 2003
- Microsoft Outlook 2003 Service Pack 2 UPDATED
- Microsoft Outlook 2003 Multilingual User Interface Packs
- Microsoft Outlook 2003 Language Interface Packs
- Microsoft Exchange Server 5.0 Service Pack 2, Service Pack 4
- Microsoft Exchange Server 5.0 Service Pack 3 with the Exchange 2000 Post-Service Pack 3 Update
- Microsoft Exchange Server 5.5 Service Pack 1, Service Pack 2, Service Pack 3, Service Pack 4

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: High

ORIGINAL DESCRIPTION:

A new vulnerability has been discovered in both the Microsoft Outlook Email Client and the Microsoft Exchange Email Server. This vulnerability exists when the affected applications decode an email message containing a specially-crafted TNEF (Transport Neutral Encapsulation Format) MIME attachment. Both Microsoft Outlook and Microsoft Exchange use the TNEF format when sending and receiving Rich Text Format (RTF) messages.

No user action is required for the successful exploitation of an affected Microsoft Exchange Server; the server must only accept a specially-crafted message. A user must open or preview the specially-crafted message for successful exploitation of an affected computer running Microsoft Outlook, but does not need to open or click on an attachment.

After successful exploitation, an attacker could take control of a vulnerable system, and perform actions such as install programs, view, change, and delete data, and create user accounts.

Microsoft has released several patches which addresses these vulnerabilities as well as several workarounds.

JAANUARY 9 UPDATED DESCRIPTION:

Three new vulnerabilities were announced for Microsoft Outlook Email Client.

The first vulnerability affects the Advanced Search Feature in Outlook. An attacker can exploit this vulnerability if an affected user opens a malformed .oss file. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. This vulnerability is rated Critical for Outlook 2000, and Important for Outlook 2002 and 2003.

The second vulnerability exists in the way that Microsoft Outlook Email Client parses email headers. An attacker who successfully exploited the vulnerability could send a malicious e-mail to an Outlook user that would cause the client to fail until the malformed e-mail was removed from the e-mail server. The e-mail message could be deleted by an e-mail administrator, or by the user via another e-mail client such as Outlook Web Access and Outlook would again function normally.

The third vulnerability exists in the way Outlook processes malformed VEVENT records. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose Outlook client is set to use MAPI with Microsoft Exchange Server are not affected due to Exchange's handling of iCal calendar data embedded in messages or in .ICS attachments.

RECOMMENDATIONS:

CSCIC recommends the following actions be taken:

- Apply all the appropriate patches provided by Microsoft to vulnerable systems as soon as possible after appropriate testing. A listing of those patches are located at:
<http://www.microsoft.com/technet/security/Bulletin/MS06-003.mspx>
- Block untrusted incoming traffic from the Internet at your network perimeter.
- Consider blocking all MS-TNEF attachments on Microsoft Exchange Server, if business needs permit, until the appropriate patches have been applied. Please note that if all MS-TNEF attachments are blocked, e-mail messages that are formatted as RTF will not be received correctly. In some cases, users could receive blank e-mail messages instead of the original RTF-formatted e-mail message. In other cases, users may not receive e-mail messages that are formatted as RTF at all.

JANUARY 9 UPDATED RECOMMENDATIONS

- **Apply all the appropriate patches provided by Microsoft to vulnerable systems as soon as possible after appropriate testing. A listing of those patches are located at:**
<http://www.microsoft.com/technet/security/Bulletin/MS07-003.mspx>.
- **Block untrusted incoming traffic from the Internet at your network perimeter.**
- **Consider blocking all .oss and .ics attachments on Microsoft Exchange Server. This may affect users that utilize and share Advanced Find searches in Outlook and calendar entries.**

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/MS06-003.mspx>

Secunia:

<http://secunia.com/advisories/18368/>

Security Focus:

<http://www.securityfocus.com/bid/16197>

JANUARY 9 UPDATED REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/MS07-003.msp>