



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

December 10, 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.

DATE(S) ISSUED:

12/10/2008

SUBJECT:

Vulnerability in WordPad Text Converter Could Allow Remote Code Execution

OVERVIEW:

A new vulnerability has been discovered in the Microsoft Windows WordPad Text Converter for the Word 97 file format that would allow a remote attacker to take complete control of the vulnerable system. The WordPad Text Converter is a component that is installed by default that allows some applications to open Word documents if Word is not installed. This vulnerability can be exploited when a user opens a specially crafted Word 97 file using WordPad. Successful exploitation may result in an attacker gaining complete control of the affected system. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete files; or create new accounts with user rights.

It should be noted that this vulnerability is currently being exploited on the Internet and there is no patch available at this time.

SYSTEMS AFFECTED:

- Windows 2000 SP4
- Windows XP SP2
- Windows XP Professional x64 Edition, SP2
- Windows 2003 Server SP1, SP2
- Windows 2003 Server for Itanium-based systems
- Windows 2003 Server x64 Edition, SP2

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**DESCRIPTION:**

A new vulnerability has been identified in the Microsoft Windows WordPad Text Converter. This vulnerability affects the WordPad Text Converter and could be exploited when a user opens a specially crafted Word 97 file (.doc, .wri, or .rtf file extensions). If Microsoft Word is installed, the .doc and the .rtf file will open by default in Word, which is not vulnerable to the exploit. However if the attacker uses the .wri file extension, the file would automatically open in WordPad. Successful exploitation may result in an attacker gaining complete control of the affected system. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete files; or create new accounts with user rights. This vulnerability cannot be automatically exploited through email. The user needs to open a malicious document.

It should be noted that this vulnerability is currently being exploited on the Internet and there is no patch available at this time.

We recommend that you follow the workaround instructions which can be found on Microsoft's website at the following location:
<http://www.microsoft.com/technet/security/advisory/960906.msp>. These instructions explain how to disable the WordPad Text Converter. This workaround will not correct the underlying vulnerability, but it will help in blocking known attack vectors.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Follow the workaround instructions for how to disable the WordPad Text Converter.
- Do not open untrusted documents using WordPad.
- Consider blocking .wri files at the network perimeter
- Do not visit unknown or un-trusted Web sites.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:**Microsoft:**

<http://www.microsoft.com/technet/security/advisory/960906.msp>

Security Focus:

<http://www.securityfocus.com/bid/32718>

Secunia:

<http://secunia.com/Advisories/32997/>

CVE

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4841>