



eSecurity Advisory

Vulnerability in Microsoft Word Could Allow Remote Code Execution

Microsoft is investigating new public reports of limited zero-day attacks using a vulnerability in Microsoft Word 2000. In order for this attack to be carried out, a user must first open a malicious Word file attached to an e-mail or otherwise provided to them by an attacker.

To determine if your version of Word is Microsoft Word 2000, first open Microsoft Word and choose Help on the Menu Bar. Then select About Microsoft Word and your version information should be displayed in the pop up box.

At this point, a patch to fix the problem has not been released.

What can you do?

Microsoft has tested the following workarounds. While these workarounds will not correct the underlying vulnerability, they help block known attack vectors.

- Do not open or save Microsoft Word files that you receive from un-trusted sources or that you receive unexpectedly from trusted sources.
- Temporarily use Word Viewer 2003 to open and view Microsoft Word files. Word Viewer 2003 does not contain the vulnerable code and is not susceptible to this attack. To download the Word Viewer 2003 for free, visit: <http://www.microsoft.com/downloads/details.aspx?familyid=95E24C87-8732-48D5-8689-AB826E7B8FDF&displaylang=en>.

Listed below is more information that may helpful to users to protect their work and home computers.

SUBJECT:

A vulnerability in Microsoft Word 2000 have been discovered which could allow Remote Code Execution.

SYSTEMS AFFECTED:

- Microsoft Word 2000

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:

Microsoft is investigating new public reports of limited “zero-day” attacks using a vulnerability in Microsoft Word 2000. In order for this attack to be carried out, a user must first open a malicious Word file attached to an e-mail or otherwise provided to them by an attacker.

Opening the Word document out of email will prompt the user to be careful about opening the attachment.

Upon completion of this investigation, Microsoft will take the appropriate action to help protect our customers. This may include providing a security update through our monthly release process or providing an out-of-cycle security update, depending on customer needs.

Microsoft has not released patches which address these vulnerabilities.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/advisory/925059.mspx>

<http://blogs.technet.com/msrc/>