

[NT] WordPerfect Converter Vulnerability Allows Code Execution (MS04-027)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0036.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/15/04

To: list@securiteam.com

Date: 15 Sep 2004 10:51:46 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

WordPerfect Converter Vulnerability Allows Code Execution (MS04-027)

SUMMARY

A remote code execution vulnerability exists in the WordPerfect Converter that is provided as part of the affected software listed below. The advisory documents the vulnerability and provides update information.

If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges. However, user interaction is required to exploit this vulnerability.

DETAILS

Vulnerable Systems:

* Microsoft Office 2000 Service Pack 3 (Word 2000, FrontPage 2000 and Publisher 2000) –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=88F52E69-99E1-4892-9A53-84E5DFADFE6B>>

Download the update

Securiteam: [NT] WordPerfect Converter Vulnerability Allows Code Execution (MS04-027)

* Microsoft Office XP Service Pack 3 (Word 2002, FrontPage 2002 and Publisher 2002) –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=10A6CEB3-7B94-4F74-A5A0-60C31CE2F57B>>

Download the update

* Microsoft Office 2003 (Word 2003, FrontPage 2003 and Publisher 2003) –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=A0629800-1889-495B-B25E-4637D6B03250>>

Download the update

* Microsoft Works Suite 2001 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=88F52E69-99E1-4892-9A53-84E5DFADFE6B>>

Download the update (same as Microsoft Office 2000 link)

* Microsoft Works Suite 2002 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=10A6CEB3-7B94-4F74-A5A0-60C31CE2F57B>>

Download the update (same as the Microsoft Office XP link)

* Microsoft Works Suite 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=10A6CEB3-7B94-4F74-A5A0-60C31CE2F57B>>

Download the update (same as the Microsoft Office XP link)

* Microsoft Works Suite 2004 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=10A6CEB3-7B94-4F74-A5A0-60C31CE2F57B>>

Download the update (same as the Microsoft Office XP link)

Affected Components:

* Microsoft WordPerfect 5.x Converter

Immune Systems:

* Microsoft Office 2003 Service Pack 1

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0573>>

CAN-2004-0573

Security Update Replacement: This update replaces the security update that was provided as part of Microsoft Security Bulletin

<<http://go.microsoft.com/fwlink/?LinkId=19386>> MS03-036.

WordPerfect Converter Code Execution Vulnerability

A remote code execution vulnerability exists in the Microsoft WordPerfect 5.x Converter. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of the affected system. However, user interaction is required to exploit this vulnerability.

Mitigating Factors For WordPerfect Converter Code Execution

* In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability.

An attacker would have no way to force users to visit a malicious Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site. After they click the link, they would be prompted to perform several actions. An attack could only occur after they performed these actions.

Securiteam: [NT] WordPerfect Converter Vulnerability Allows Code Execution (MS04–027)

* The vulnerability cannot be exploited automatically through e–mail. A user must open an attachment this is sent in an e–mail message for an attack to be successful through e–mail.

* An attacker who successfully exploited this vulnerability could gain the same privileges as the user. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

* This vulnerability does not affect WordPerfect 6.x documents, which are handled by a separate converter (wpft632.cnv).

Workarounds For WordPerfect Converter Code Execution

* Do not open WordPerfect 5.x documents from untrusted sources using any software listed as affected in this bulletin on systems that are not updated with the security updates that accompany this bulletin.

* Uninstall the WordPerfect 5.x Converter from your system through Add or Remove Programs. Choose a program from the Affected Software list that is installed on your system and click Change. The WordPerfect 5.x Converter is an Office Shared Feature.

Impact of workaround: Opening WordPerfect 5.x documents using any software listed in the Affected Software section would no longer be possible.

* Use a third–party WordPerfect 5.x to Word converter or ask the user of WordPerfect to save the document in another format.

Frequently Asked Questions For WordPerfect Converter Code Execution

What is the scope of the vulnerability ?

This is a remote code execution vulnerability. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

What causes the vulnerability ?

An unchecked buffer in the Office WordPerfect 5.x Converter.

What is the Microsoft Office WordPerfect 5.x Converter ?

The Microsoft Office WordPerfect 5.x Converter helps users convert documents from Corel WordPerfect 5.x file formats to Microsoft Word file formats. The WordPerfect 5.x Converter is included in all versions of Office and is also available separately in the Office Converter Pack. However, user interaction is required to exploit this vulnerability.

What is the Microsoft Office Converter Pack ?

The Microsoft Office Converter Pack combines file converters and filters that were not included in earlier versions of Office. These converters and filters allow Office to use additional document formats that were not

Securiteam: [NT] WordPerfect Converter Vulnerability Allows Code Execution (MS04-027)

natively supported. The Office Converter Pack is available
<<http://go.microsoft.com/fwlink/?LinkId=34318>> as a Web download.

What might an attacker use the vulnerability to do ?

An attacker who successfully exploited this vulnerability could take any action on a user's system that the user had permissions to carry out.

How could an attacker exploit the vulnerability ?

An attacker could exploit the vulnerability by sending a malicious file to the user and by persuading the user to open the file. If the user opened the file, the application that used the WordPerfect 5.x Converter could fail and could allow the attacker to execute code of their choice.

Can the vulnerability be exploited automatically through an e-mail message ?

No. A user must open a malicious document that an attacker provided in order for the vulnerability to be exploited. Viewing an e-mail message, even if Microsoft Word had been selected as the default e-mail editor for Microsoft Outlook, would not expose the vulnerability.

Is the Microsoft Office WordPerfect 5.x Converter installed by default in all software listed in the "Affected Software" section of this bulletin ?

Yes. By default, the WordPerfect 5.x Converter is installed in all supported versions of the software listed in the Affected Software section of this bulletin. However, the user has the ability to not install the converter during the setup process.

What systems are primarily at risk from the vulnerability ?

Workstations and terminal servers are primarily at risk. Servers are only at risk if users who do not have sufficient administrative credentials are given the ability to log on to servers and to run programs. However, best practices strongly discourage allowing this.

What does the update do ?

The update removes the vulnerability by modifying the way that the WordPerfect 5.x Converter validates the length of a message before it passes the message to the allocated buffer.

When this security bulletin was issued, had this vulnerability been publicly disclosed ?

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information indicating that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited ?

No. Microsoft had not received any information indicating that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

Securiteam: [NT] WordPerfect Converter Vulnerability Allows Code Execution (MS04-027)

ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/ms04-027.msp>>

<http://www.microsoft.com/technet/security/bulletin/ms04-027.msp>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.