

# [NT] Unchecked buffer in Microsoft Access Snapshot Viewer Could Allow Code Execution

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0006.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 09/04/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 4 Sep 2003 10:17:28 +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>

-----

Unchecked buffer in Microsoft Access Snapshot Viewer Could Allow Code Execution

---

## SUMMARY

With Microsoft Access Snapshot Viewer, you can distribute a snapshot of a Microsoft Access database that allows the snapshot to be viewed without having Access installed. For example, a customer may want to send a supplier an invoice that is generated by using an Access database. With Microsoft Access Snapshot Viewer, the customer can package the database so that the supplier can view it and print it without having Access installed. The Microsoft Access Snapshot Viewer is available with all versions of Access – though it is not installed by default – and is available as a separate stand-alone download. The Snapshot Viewer is implemented by using an ActiveX control.

A vulnerability exists because of a flaw in the way that Snapshot Viewer validates parameters. Because the parameters are not correctly checked, a buffer overrun can occur, which could allow an attacker to execute the code of their choice in the security context of the logged-on user.

For an attack to be successful, an attacker would have to persuade a user to visit a malicious Web site that is under the attacker's control.

## Securiteam: [NT] Unchecked buffer in Microsoft Access Snapshot Viewer Could Allow Code Execution

### DETAILS

#### Affected Software:

- \* Microsoft Access 97
- \* Microsoft Access 2000
- \* Microsoft Access 2002

#### Mitigating factors:

- \* The Microsoft Access Snapshot Viewer is not installed with Microsoft Office by default.
- \* An attacker would need to persuade a user to visit a website under the attacker's control for an attack to be successful.
- \* An attacker's code would run with the same permissions as the user. If a user's permissions were restricted, the attacker would be similarly restricted.

#### Patch availability:

Download locations for this patch

#### Access 2002:

~~<<http://microsoft.com/downloads/details.aspx?FamilyId=B50D4863-1BBE-4009-9DF8-52D3A916D54F&displaylan>~~  
~~<http://microsoft.com/downloads/details.aspx?FamilyId=B50D4863-1BBE-4009-9DF8-52D3A916D54F&displaylan>~~

<<http://microsoft.com/office/ork/xp/journ/snpv1001a.htm>>  
<http://microsoft.com/office/ork/xp/journ/snpv1001a.htm> (administrative update only)

#### Access 2000:

<<http://microsoft.com/downloads/details.aspx?FamilyId=F6CB9C8E-16E3-422D-86DD-7ED5671FB8D4&displaylan>

<<http://microsoft.com/office/ork/2000/journ/snpv0901.htm>>  
<http://microsoft.com/office/ork/2000/journ/snpv0901.htm> (administrative update only)

#### Access 97:

Install the updated stand-alone Snapshot Viewer control. To do so, visit the following Microsoft Web site:

<<http://www.microsoft.com/AccessDev/Articles/snapshot.htm>>  
<http://www.microsoft.com/AccessDev/Articles/snapshot.htm>

#### Stand-alone Snapshot Viewer Control:

<<http://www.microsoft.com/AccessDev/Articles/snapshot.htm>>  
<http://www.microsoft.com/AccessDev/Articles/snapshot.htm>

#### What's the scope of the vulnerability?

This is a buffer-overflow vulnerability. An attacker who successfully exploited this vulnerability could run programs on another user's system. Such a program could take any action that the user could take, such as

## Securiteam: [NT] Unchecked buffer in Microsoft Access Snapshot Viewer Could Allow Code Execution

adding, changing, or deleting any data or configuration information. For example, the code could lower the security settings in the browser or write a file to the hard disk. Because the code would run as the user and not as the operating system, any security limitations on the user's account would also be applicable to any code that is run by successfully exploiting this vulnerability. In environments where user accounts are restricted, such as enterprise environments, the actions that an attacker's code could take would be limited by these restrictions.

What causes the vulnerability?

The vulnerability results because of an unchecked buffer in the ActiveX control that Microsoft Access Snapshot Viewer uses. By invoking a specific function in a particular manner, an attacker could overflow the buffer and gain the ability to run code in the user's security context.

What is the Microsoft Access Snapshot Viewer?

The Microsoft Access Snapshot Viewer, you can distribute a snapshot of a Microsoft Access database that allows the snapshot to be viewed without having Access installed. For example, a customer may want to send a supplier an invoice that is generated by using an Access database – the Snapshot viewer would allow the customer to package the database. With Microsoft Access Snapshot Viewer, the supplier can view it and print it without having Access installed.

The Microsoft Access Snapshot Viewer is available with all versions of Microsoft Office – though it is not installed by default – and is available as a separate stand-alone download. The Snapshot Viewer is implemented by using an ActiveX control.

What is an ActiveX control?

ActiveX is a technology that allows developers to deploy programs in a small, self-contained way. These programs are called controls and can be used by Web pages, Visual Basic programs, or other applications.

ActiveX controls can be distributed in several ways, including installing with software products or being offered for download from a Web site. Regardless of how a user installs an ActiveX control, after it is installed and registered on the user's system it is fully functional and available to the user.

How could I get the ActiveX control that Microsoft Access Snapshot Viewer uses?

There are several ways to get the Microsoft Access Snapshot Viewer:

- \* It is included with all supported versions of Access – however it is not installed by default.
- \* It is available as a separate stand-alone download so that customers who do not have Access installed can view Access database snapshots.

What is wrong with the ActiveX control that Microsoft Access Snapshot Viewer uses?

## Securiteam: [NT] Unchecked buffer in Microsoft Access Snapshot Viewer Could Allow Code Execution

There is an unchecked buffer in one of the functions that handles the input of certain parameters to the control.

What could this vulnerability enable an attacker to do?

This vulnerability could enable an attacker to run the code of their choice on a user's system with the same level of permissions as the user. This could allow the attacker to carry out any action that the user can carry out, such as adding, changing, or deleting data, communicating with a Web site, or formatting the hard disk.

How could an attacker exploit the vulnerability?

There are several ways that an attacker could exploit the vulnerability:

- \* The attacker could host a page on a Web site that they control. If a user visited the site and opened the Web page, the page would try to invoke the control.

- \* The attacker could send a link to a malicious Web page in an e-mail message. If the recipient clicked the link, the Web page would try to invoke a control on the malicious Web site.

Could the old control still be downloaded?

If an attacker has cached the old vulnerable control and is hosting it on a site that is under their control, the control could be reintroduced to a user's system. However, an attacker would have to persuade a user to visit a malicious Web site that is under their control for the user to download the old control.

To remove the ability for the old control to be reintroduced on a user's system, a kill bit will be issued for the old control in a forthcoming Internet Explorer security patch.

What is a kill bit?

There is a security feature in Microsoft Internet Explorer that makes it possible to prevent an ActiveX control from ever being loaded by the Internet Explorer HTML-rendering engine. This is done by making a registry setting and is referred to as setting the kill bit. After the kill bit is set, the control can never be loaded, even when it is fully installed. Setting the kill bit makes sure that even if a vulnerable component is introduced or is re-introduced to a system, it remains inert and harmless. For more information about this feature, see the following Microsoft Knowledge Base article: 240797.

What does the patch do?

The patch eliminates the vulnerability by making sure that the Microsoft Access Snapshot Viewer ActiveX control correctly validates the parameters that are sent to the affected function. Additionally, the stand-alone download for Microsoft Access Snapshot Viewer has been updated with the same revised version of the ActiveX control.

ADDITIONAL INFORMATION

Securiteam: [NT] Unchecked buffer in Microsoft Access Snapshot Viewer Could Allow Code Execution

The information has been provided by

<mailto:0\_51916\_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C\_US@Newsletters.Microsoft.com>

Microsoft Product Security.

=====

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.