

[NT] Remotely Exploitable Buffer Overruns in Microsoft's Commerce Server 2000/2

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0014.html>

From: support@securiteam.com

Date: 07/07/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 7 Jul 2002 00:37:57 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Remotely Exploitable Buffer Overruns in Microsoft's Commerce Server 2000/2

SUMMARY

Microsoft's Commerce Server 2000 and 2002 are web server products for building e-commerce sites. These products provide tools and features that simplify the development and deployment of e-commerce solutions and analyzing site usage and performance. There are several remotely exploitable buffer overruns in Commerce Server in disparate locations and a CGI executable that allows the execution of arbitrary commands.

DETAILS

Vulnerable systems:

- * WinNT
- * Win2K
- * WinXP

The Profile Service of Microsoft Commerce Server 2000 allows remote attackers to cause the server to fail or run arbitrary attacker supplied code in the security context of the Local SYSTEM account. Several areas in this service contain vulnerable code.

Securiteam: [NT] Remotely Exploitable Buffer Overruns in Microsoft's Commerce Server 2000/2

The Office Web Components (OWC) package installer used by Microsoft Commerce Server 2000 allows remote attackers to cause the process to run arbitrary code in the LocalSystem security context by via input to the OWC package installer. By default, users have to authenticate to access this executable so the risk posed is less severe in nature.

Again, the Office Web Components (OWC) package installer for Microsoft Commerce Server 2000 allows remote attackers to execute commands by passing the commands as input to the OWC package installer with a '/C' option.

Fix Information:

NGSSoftware alerted Microsoft to these problems on the 6th March 2002. The patches are available from:

* Microsoft Commerce Server 2000:

<<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=39591>>
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=39591>

* Microsoft Commerce Server 2002:

<<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=39550>>
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=39550>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:nisr@nextgenss.com>>
NGSSoftware Insight Security Research.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NT] Argosoft Mail Server Plus/Pro Webmail Reverse Directory Traversal"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)