

Alert: Microsoft Security Bulletin – MS02–049

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2002-09/0001.html>

From: Russ (Russ.Cooper@RC.ON.CA)

Date: 09/04/02

Date: Wed, 4 Sep 2002 14:30:52 -0400

From: Russ <Russ.Cooper@RC.ON.CA>

To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

<http://www.microsoft.com/technet/security/bulletin/MS02-049.asp>

Flaw Could Enable Web Page to Launch Visual FoxPro 6.0 Application Without Warning (Q326568)

Originally posted: September 04, 2002

Summary

Who should read this bulletin: Customers using Microsoft® Visual FoxPro 6.0

Impact of vulnerability: Attacker could gain control over user's system.

Maximum Severity Rating: Moderate.

Recommendation: Customers using Visual FoxPro 6.0 should install the patch immediately.

Affected Software:

– Microsoft Visual FoxPro 6.0

Technical description:

In general, when an product installs, it should register itself with Internet Explorer. This allows the product to specify how Internet Explorer should handle files associated with it when referenced from a web page – for instance, it allows the product to specify whether the user should be presented with a warning dialogue before such a file is opened.

Visual FoxPro 6.0 does not perform this registration, and this gives rise to a situation in which a web page could automatically launch a Visual FoxPro application (i.e., an .app file). In most cases, this would not result in a security vulnerability – because of the way Visual FoxPro 6.0 evaluates file names, FoxPro itself could be started but the .app file would typically not run. However, if the filename of the application were constructed in a particular way, a second error (associated with how Visual FoxPro 6.0 evaluates application filenames) could not only start FoxPro but allow the application to execute.

The vulnerability could be exploited by creating a web page that references a Visual FoxPro application, and either hosting it on a web site or sending it to a user as an HTML mail. If the user had installed Visual FoxPro 6.0 – or had installed a product that includes the Visual FoxPro 6.0 runtime – and the filename of the

NT-Bugtraq: Alert: Microsoft Security Bulletin – MS02–049

application was constructed in a particular way, the application would execute. This would enable the application to not only interrogate databases, but also issue system commands in the user's security context.

Mitigating factors:

- The vulnerability could only be exploited if Visual FoxPro 6.0 (or the Visual FoxPro 6.0 runtime) is installed on the system. Other products, and other versions of Visual FoxPro, are not affected by the vulnerability.
- The most privileges the application could gain would be those of the user. If the user were operating in a less-privileged context, it would limit the damage that the application could cause.

Vulnerability identifier: CVE–CAN–2002–0696

This email is sent to NTBugtraq automatically as a service to my subscribers. Since its programmatically created, and since its been a long time since anyone paid actual money for my programming skills, it may or may not look that good...;-]

I can only hope that the information it does contain can be read well enough to serve its purpose.

Cheers,

Russ – Surgeon General of TruSecure Corporation/NTBugtraq Editor

- ***Previous message:*** [NGSSoftware Insight Security Research: "Microsoft SQL Server Stored procedures \[sp_MSSetServerPropertiesn and sp_MSsetalertinfo\] \(#NISR03092002A\)"](#)
- ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)