

# MSIE 6.0 will rollback during XP Pro Install -- Ref: MSIE may download and run programs automatically – details

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-01/0202.html>

---

**From:** Jeffrey W. Dronenburg ([dronenjw@gmpexpress.net](mailto:dronenjw@gmpexpress.net))

**Date:** 01/15/02

From: "Jeffrey W. Dronenburg" <[dronenjw@gmpexpress.net](mailto:dronenjw@gmpexpress.net)>

To: <[bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)>

Date: Tue, 15 Jan 2002 03:07:07 -0500

**Title:**

Microsoft Internet Explorer 6.0 files will rollback during installation of Windows XP Pro Upgrade Version

**Known Systems Affected:**

- Windows XP Professional Upgrade Version 2002 (Windows XP Home Upgrade NOT tested)
- Internet Explorer Version 6.0.2600.0000 Update Patches; Q313675;

**Risk:** High (from the original MS Release)

- Internet systems: Critical
- Intranet systems: Critical
- Client systems: Critical

**Date:** January 15, 2002

Jeffrey Dronenburg Advisory: #01-2002

\_\_\_\_\_=====+++(\*)+++=====\_\_\_\_\_

**Synopsis:**

1) When upgrading to Windows XP Pro from previous versions of Windows (only Win 98SE validated), IE 6.0 files are overwritten during the operating system software installation process, effectively rolling the browser software back to original release version 6.0.0000.0000 and removing all installed patches, including Q313675 (See MS01-058).

2) The Microsoft Windows Update web site for XP Pro <http://v4.windowsupdate.microsoft.com/en/default.asp> will not detect Internet Explorer or recommend update patches.

\_\_\_\_\_=====+++(\*)+++=====\_\_\_\_\_

Notification:

\* Submitted to Microsoft Feedback

<http://support.microsoft.com/default.aspx?scid=fh:EN-US:FEEDBACK> for Site Content, Features, and Tools on 1/15/2002 at 1:25 AM EST. Vendor alerted immediately upon discovery of vulnerability. Vendor additionally notified of this BUGTRAQ e-mail submission and provided with text of details.

\* Submitted to BUGTRAQ immediately without waiting for vendor response to further document this serious, already well known potential security breach. The particular vulnerability discussed in this advisory may arise out of a false sense of security created by taking normal security precautions and installing system patches following standard, vendor recommended procedures (i.e. update all application software prior to OS upgrade).

\_\_\_\_\_=====+++(\*)+++=====\_\_\_\_\_

Details:

I had previously installed the MS01-058 cumulative patch for IE 6.0 from the MS TechNet web site when it was first released to BUGTRAQ by the Microsoft Security Notification Service last month (13 December 2001). Since then, I have installed the upgrade version of Windows XP Pro from Windows 98SE (please don't debate the wisdom of doing this with me). Remember, I thought that my IE 6.0 configuration was fully patched, and I didn't give it another thought (mistake #1).

After installing XP Pro, I went to the Windows Update site and installed all available security patches using auto detection, including the UPnP vulnerability patch. At this point I \*assumed\* I had a completely patched operating system (mistake #2 -- something about an old adage when you ass\*u\*me things).

Tonight, I went to the Online Solutions web site linked in Jouko Pynnonen's e-mail thread quoted below and was \*surprised\* -- \*stunned\* -- when the test revealed a vulnerable browser. I immediately clicked on About Internet Explorer and was completely surprised to find version 6.0.0000.0000. No patches! Evidently, the XP Pro installation must have erased all IE 6.0 patched files and replaced them with original release files.

I went back to the Windows Update site for XP Pro and the site again \*failed to detect\* any missing patches for IE. No critical patches were identified. Evidently, IE 6.0 isn't included in the self-detect on this site as it is on the Windows 98 Update site. I then went to the TechNet security page detailing MS01-058 and reinstalled the patch. Testing passed on the Online Solutions test page linked below.

Thank you again, Jouko and Online Solutions for providing this very timely online tool and reminder to test our browsers!

\_\_\_\_\_=====+++(\*)+++=====\_\_\_\_\_

Workaround/Solutions:

- 1) Validate current version of Internet Explorer by clicking on Help -> About Internet Explorer and ensure that Update Patches:; Q313675; is reflected.
- 2) Test Internet Explorer on the Online Solutions Web site at <http://www.solutions.fi/iebug2>.
- 3) If required: - A patch is available to fix this vulnerability. Please read the Microsoft Security Bulletin at <http://www.microsoft.com/technet/security/bulletin/ms01-058.asp> for vendor information on obtaining this patch.
- 4) Subscribe to the Microsoft Product Security Notification Service e-mail notification list. This may be the only reliable way to be kept apprised of critical patches and updates to IE from Microsoft until Windows Update is modified.

\_\_\_\_\_=====+++(\*)+++=====\_\_\_\_\_

<!-- onSoapBox -->

For the Microsoft personnel screening BUGTRAQ:

PLEASE (all caps added for emphasis) include IE on the Windows XP Pro Update site (<http://v4.windowsupdate.microsoft.com/en/default.asp>). Your customers should not have to go to [www.anysite.fi](http://www.anysite.fi) to validate the current patch status of your software products. Of all of the controversies surrounding the current release of the XP operating system, this specific issue is particularly reprehensible and annoying.

Your developers put together a great tool to determine system software status and assist your customers in selecting appropriate updates and patches for their systems. Perhaps too great a tool, as it has become an assumption crutch. I happen to be in that <1% of the Windows users population that follows developments in software security (and the BUGTRAQ mailing list along with other SecurityFocus.com lists). What about the remaining 99%? They depend on tools like Windows Update to keep their systems, well, up to date (if they even do that). IMHO, the tool is broken until it fully detects all system updates and patches for your software products, or at least points you to the tool that will (like the Office Update site).

<!-- offSoapBox -->

\_\_\_\_\_=====+++(\*)+++=====\_\_\_\_\_

Lessons Learned:

Don't rely on vendor supplied automated tools -- check your system thoroughly after any operating system upgrade. Then, check it again. One more time for a confidence check. Repeat continuously.

SecurityFocus Bugtraq: MSIE 6.0 will rollback during XP Pro Install -- Ref: MSIE may download and run programs automatically

<!-- That must be in a Systems Security 101 book somewhere... -->

Cheers,

Jeffrey Dronenburg, Sr.  
MIS Major, Univ. of Maryland, Univ. College  
Alpha Sigma Lambda  
Phi Kappa Phi

"A day without learning is like apple pie without ice cream. They're both much sweeter the other way around." --Me! :-)

P.S. Tonight, I learned another lesson in systems security thanks to the BUGTRAQ...

\_\_\_\_\_=====+++(\*)+++=====\_\_\_\_\_

The Fine Print:

Legal Notice:

This Advisory is Copyright (c) 2002 Jeffrey W. Dronenburg, Sr.  
You may distribute it unmodified. When replying to this advisory, you may omit certain sections as long as it does not change the meaning or intent of the advisory, and the omitted sections are replaced with "<snip>". You may not otherwise modify it for distribution, or distribute parts of it without the author's written permission.

Disclaimer:

The information in this advisory is believed to be true based on my own experiments though it may be proven to be invalid. If you discover through continued experimentation that the results of my own experiments are not valid, please do me the professional courtesy of informing me of your findings, and copying me when posting to mailing lists such as SecurityFocus.com's BUGTRAQ.

The opinions expressed in this advisory are my own and not of any government agency or company. The usual standard disclaimers apply, especially the fact that Jeffrey W. Dronenburg, Sr. is not liable for any damages caused by the direct or indirect use of the information provided by this advisory. The information in this advisory is being released to the Information Systems and Network Security Community as a whole in the interest of furthering computer systems security. Jeffrey W. Dronenburg, Sr. bears no responsibility for the content or misuse of the information provided in this advisory or any derivatives thereof.

----- End of Message -----

----- Portions of Original Quoted Message from BUGTRAQ -----

From: "Jouko Pynnonen" <[jouko@solutions.fi](mailto:jouko@solutions.fi)>  
To: <[bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)>  
Sent: Monday, January 14, 2002 8:58 AM  
Subject: MSIE may download and run programs automatically -- details

MSIE 6.0 will rollback during XP Pro Install -- Ref: MSIE may download and run programs automatically --

This posting briefly describes some technical details of the vulnerability discussed in the Bugtraq messages with the subjects "MSIE may download and run programs automatically" (Dec 14 2001) and "File extensions spoofable in MSIE download dialog" (Nov 26 2001).

<snip>

If you want to check if your browser is vulnerable, you can do it on this web page:

<http://www.solutions.fi/iebug2>

After clicking the link there, a vulnerable IE will download a small program and run it. The program will run in a DOS window and print a message. If this happens, you should patch your browser. The patch has been available since 13 December 2001 at Microsoft's site:

<http://www.microsoft.com/technet/security/bulletin/MS01-058.asp>

A non-vulnerable IE will show a download dialog with a filename ending with ".EXE".

--

Jouko Pynnonen  
[jouko@solutions.fi](mailto:jouko@solutions.fi)

Online Solutions Ltd  
<http://www.solutions.fi>

Secure your Linux -  
<http://www.secmod.com>

- 
- **Previous message:** [bugzilla@redhat.com](mailto:bugzilla@redhat.com): "[RHSA-2002:013-03] Updated sudo package is available"
  - **In reply to:** [Jouko Pynnonen: "MSIE may download and run programs automatically - details"](#)
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)