



- CATEGORIES
- Home
- About Security Watch
- Apple
- DNS
- Domain Issues
- E-Commerce
- E-Mail
- Firefox
- Hacking
- Identity
- Internet Crime
- Internet Explorer
- Linux/Unix
- Malware
- Mobile Security
- Networking
- News
- Office
- Phish
- Privacy
- Security Software
- Servers
- Social Media
- Software Patches
- Spam
- Top Threat
- Vulnerabilities
- Windows 7
- Windows Vista
- Windows XP
- Wireless

OUR NEWSLETTERS

Subscribe to Security Watch  
 Our FREE email newsletter delivered to your inbox.  
 Email:

Format: HTML



RSS FEEDS

Never miss a story. Add our RSS Feed to your favorite feed reader.

- XML
- MY YAHOO!
- Add to Google
- MY MSN
- MY AOL
- Reyz
- newsgator
- Bloglines
- Technorati
- Windows Live

CONTACT US

Got a Question?

Monday March 29, 2010

### Analysis Shows Value of Standard User Accounts Against Vulnerabilities

Categories: Apple, Hacking, Internet Explorer, Linux/Unix, Malware, Office, Security Software, Servers, Software Patches, Top Threat, Vulnerabilities, Windows 7, Windows Vista, Windows XP

Tags: exploit, malware, patch, privilege, update, vulnerability

One of the most important general guidelines you can follow in order to keep your systems secure is to run your users and programs with a "least privilege" philosophy. In practice for Windows users, the most important example of this is not to run users as administrator, but as a standard user.



[A study just released by BeyondTrust shows some of the value of this approach in mitigating the impact of reported vulnerabilities in Microsoft products.](#) It's common to find a disclosed vulnerability in a Microsoft product to be less severe, if at all an issue, when the user in whose context the exploit runs, is logged on with limited privileges. The study shows just how common.

100% of Microsoft Office vulnerabilities reported in 2009 were mitigated by running as standard user. Office 2010 will take this approach a step further, incidentally, with [Protected View](#), a special low-privileged and sandboxed mode for viewing documents coming from untrusted sources. 100% of Internet Explorer 8 vulnerabilities reported in 2009 and 94% of all IE vulnerabilities last year were mitigated by running as standard user. Of all Microsoft vulnerabilities disclosed in 2009, 64% were mitigated by running as standard user.

BeyondTrust makes a software solution called BeyondTrust Privilege Manager which assists administrators in allowing users to run applications, processes and even ActiveX controls with the least privilege necessary. Administrators can attach permission levels to applications and approve users for those applications, removing the need to grant them excessive permission in situations where it is not necessary. Privilege Manager works as an extension to Windows Group Policy management.

Least privilege is not just about vulnerabilities. It's also the best defense against the most common forms of malware spread by social networking. Users with standard permissions can't install applications that modify "machine" registry settings or install files in the \Windows directory, as malware is apt to do. All this is why Windows has nudged users, since the release of Vista, to run as standard user.

Like any good security practice, least privilege is not a panacea. It's possible to write malware or vulnerability exploits that do undesirable things all from user mode. A user mode program can, for example, send spam. But as a practical matter, this is very rare. Malware and exploits are designed to run in the sadly all too common scenario of the Windows user running as administrator. This is why you need to do things the smart way, and not run as admin.



Posted By: [Larry Seltzer](#)

Comments (0)

Tell a friend about this post

Post a Comment

#### WHAT DO YOU THINK?

\* = required

Name:\*

Email Address:\*

#### Ads By Google

[What's this?](#)

##### Mitigating Security Risk

Easy Log Mgmt. Compliance Solutions Free Gartner Magic Quadrant Report  
[www.RSA.com](http://www.RSA.com)

##### Enterprise Security Mgmt

Protect Your Data & Mitigate Risks. Watch the Webcast to Learn More.  
[www.ca.com](http://www.ca.com)

##### Vulnerability Scan

Is your wireless network secure? free Network Vulnerability Scan.  
[vulnerability.scan.qualys.com](http://vulnerability.scan.qualys.com)

##### Internet Security Scan

Free Malware Scan. Multiple Winner of Best Anti-Malware. Rated 5 Stars  
[www.pctools.com](http://www.pctools.com)

##### A (Ruby) Job You'll Love

Disrupt An Industry With Clean Code 400% YoY Revenue Growth - Jump In  
[www.BookRenter.com/jobs](http://www.BookRenter.com/jobs)