



March 31, 2010 Hot topics : [desktop security](#) [network security](#) [Trojans](#) [malware](#) [wpa sec](#)

Free Newsletters : [Security Daily](#)

[eSecurityPlanet.com](#) [Features](#) [All Features»](#)

Service providers can build the foundation for the next-generation Internet. See what's possible with the Cisco CRS-3, delivering 3x the scale and 2x the service intelligence.

Want PC Security? Remove Admin Rights

March 29, 2010

By [Stuart J. Johnston](#)

[Submit Feedback](#)

[»](#)

[More by Author »](#)

A new survey of Microsoft security vulnerabilities shows that the vast majority of them can be effectively mitigated while users wait for systems managers to apply the software giant's monthly patches.

The third-party report, compiled by privileged access lifecycle management vendor [BeyondTrust](#), claims that the cure for many ills that might befall users of PCs running Microsoft (NASDAQ: MSFT) software is straightforward.

"Key findings from this report show that removing administrator rights will better protect companies," said the study, dubbed [BeyondTrust 2009 Microsoft Vulnerability Analysis](#).

Administrative rights include the authority for someone designated as the system administrator to control what software and hardware can be installed on a user's PC. Often, however, the default setting is to let the user have administrative rights on his or her own PC but, as noted in the report, that can be risky because, for instance, a piece of malware might trick the system to prompt a user with such rights to okay its installation.

"By removing the need to grant administrative rights to end-users, IT departments eliminate what is otherwise the Achilles' heel of the desktop -- end-users with administrative power that can be exploited by malware and malicious intent to change security settings and disable other security solutions," the report said.

Microsoft itself frequently recommends that administrative privileges be disabled for most users.

"If a user is logged on with administrative user rights, an attacker could take complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights," a boiler plate statement reads in most Microsoft Security Bulletins.

Suspending administrative rights for most users can help block -- or, in some cases, mitigate -- many common methods of exploiting security vulnerabilities.

Related Articles

[Security Flaw Found in Broadcom NetXtreme Cards](#)

For example, the report said, eliminating administrator privileges from Windows 7 PCs -- thus blocking users from engaging in some risky activities, such as installing applications brought in from home -- would block 90 percent, or nine out of ten, of the "critical" security flaws

- [Email Article](#)
- [Print Article](#)
- [Comment on this article](#)
- [Share Articles](#)

Learn Forefront

[Create a Seamless Remote Experience with Forefront UAG](#)
Remote access solutions are often built on products from numerous vendors, creating a headache for IT managers trying to support secure network access for employees and partners. Microsoft has a solution that can help.

[Modernize your Web Security](#)
Here are some of the key reasons to switch from your existing solution(s) to Forefront Threat Management Gateway 2010.

[More Secure Web Access and Protection with Forefront TMG](#)
Forefront Product Unit Manager David Cross talks about the new Threat Management Gateway 2010 release.

[Click Here for more Forefront Resources](#)

identified since the system shipped last year.

- ▶ [BeyondTrust Extends Vista Security](#)
- ▶ [Microsoft Patch Tuesday Includes IE Warning](#)
- ▶ [Microsoft Warns on Help File Threat](#)

Additionally, removing administrative rights from users' PCs would protect against exploitation of all 55 of the vulnerabilities reported in Microsoft Office during 2009.

Similar results can be obtained by disabling administrative rights in Internet Explorer 8 -- although that is not true of earlier IE releases.

"100 percent of the Internet Explorer 8 vulnerabilities can be mitigated by removing administrator rights," the report said.

For all versions of IE, of the 33 vulnerabilities that Microsoft identified in 2009, 94 percent could be mitigated by shutting down administrative rights.

Further, configuring users without administrative privileges would protect against 81 percent of the 80 security vulnerabilities rated as "critical" -- the highest ranking in Microsoft's four-tiered severity scale, according to the study.

While systems administrators can configure users' capabilities using a variety of tools, [BeyondTrust](#) -- perhaps not surprisingly -- sells its own tool called Privilege Manager, which has been on the market since 2004.

In order to compile the report, BeyondTrust examined all of the [Security Bulletins issued by Microsoft in 2009](#) -- a total of 75 bulletins accounting for nearly 200 bug fixes.

Stuart J. Johnston is a contributing writer at [InternetNews.com](#), the news service of [Internet.com](#), the network for technology professionals.

On the Forums

[Visit the Forums »](#)

Latest

Most Views

Most Replies

How to design ITIL-CMDB schema
Today 12:02 PM by thirumaran

IT On Call Allowances
3-29-2010 06:12 PM by stevenmahoney

Cloud Computing
3-29-2010 01:11 PM by sb1

Partners

IT Legal Contracts
prepaid calling card
Boat Donations
Laptops
IP Services
Business Email
Televisions
Colocation
PDA Phones & Cases
prepaid phone card
Liability Insurance

More IT Management

CIO Update
Datamation
eSecurity Planet
ITSMWatch
Intranet Journal
IT Career Planet
Project Manager Planet
Security Definitions