Avecto

2014 Microsoft Vulnerabilities Report

Executive summary

Now in its second year, the 2014 Microsoft Vulnerabilities Report, compiled by security software company Avecto, analyses the data from Patch Tuesday Security Bulletins issued by Microsoft throughout 2014. Typically issued on the second Tuesday of each month, Patch Tuesday bulletins contain fixes for vulnerabilities affecting Microsoft products. Network administrators, Security Managers and IT Professionals then respond as quickly as they are able, ensuring the patches are rolled out across their systems to protect against the known vulnerabilities.

Key findings from the 2014 report:

Removal of admin rights key to improving security posture

The 2014 Microsoft Vulnerabilities Report once again highlights how a significant number of Critical vulnerabilities could be mitigated by the removal of user admin rights. In total, 97% of Critical vulnerabilities could be prevented from executing by simply removing admin rights across the enterprise.

The attack surface is growing

The sheer volume and increasing sophistication of cyber threats is reflected in this year's study. In the space of a year, there was a 63% increase in the number of vulnerabilities reported by Microsoft.

Closing the door on web-borne threats

The internet is widely recognized as the greatest window of opportunity for malware to enter the network. The 2014 Microsoft Vulnerabilities Report underlines how the removal of admin rights is an effective way to mitigate the threats organizations are exposed to via the browser, providing a solid security foundation on which to build defense in depth. A total of 99.5% of vulnerabilities could be managed by the removal of admin rights alone.

Recommendations

The findings from the 2014 Microsoft Vulnerabilities Report serve as another reminder as to the importance of removing admin rights in an enterprise setting. The research supports the recommendations from respected industry bodies including SANS and The Council on Cyber Security, as well as The Australian Department of Defense, who list the controlled use of administrative privileges as a fundamental part of their security best practice guidelines.

One of the most effective ways to meet the recommendations of these industry bodies is to remove administrator rights from users completely, using **Privilege Management** and **Application Control** technology to allow all users to function effectively under a standard user account.

Complement this by layering security strategies as part of a **defense in depth (DiD)** approach. The overlap of these layers of defense aim to ensure that the shortcomings of one security control are covered by another. For example, in the gap between a patch being discovered and applied, **Sandboxing** technology will trap and contain online threats so that data remains secure.

For detailed analysis and a breakdown of the statistics, download the full 2014 Microsoft Vulnerabilities Report from www.avecto.com

UK

Hobart House
Cheadle Royal Business Park
Cheadle, Cheshire, SK8 3SR

Phone +44 (0) 845 519 0114
Fax +44 (0) 845 519 0115

Americas

125 Cambridge Park Drive
Suite 301, Cambridge, MA 02140
USA

Phone 978 703 4169
Fax 978 910 0448

Australia

Level 8
350 Collins Street, Melbourne,
Victoria 3000, Australia

Phone +613 8605 4822
Fax +613 8601 1180

Avecto
@avecto
+Avecto
avecto.com
info@avecto.com