

---

**Secunia Vulnerability Study**

**Summary and Analysis**

**01/15/07**

---

## I. Core Analysis

### *Overview and Methodology*

This paper compares the security of Red Hat Enterprise Linux ES 3, Red Hat Enterprise Linux ES 4, and Microsoft Windows Server 2003 Enterprise Edition. Different aspects of operating system security, such as number of vulnerabilities and the time to resolve them, were analyzed as indicators of security for each operating system. Data collection and analysis for this study was performed in December 2006.

Data was collected from Secunia (<http://secunia.com>), a leading independent source of vulnerability intelligence. Secunia was used because they do not rely on a single source for vulnerability information, and their source data is highly transparent. Secunia not only performs their own security research but also collects and verifies security bulletins and announcements from a large base of external sources: vendors, internet forums, newsletters, security analyst bug reports, CERT, and web sites maintained by unaffiliated individuals who are tracking security issues for each platform.<sup>1</sup> For each operating system, Secunia tracks all vulnerabilities that affect a full installation of all components and packages included in the current release.<sup>2</sup>

For each vulnerability, data on start and patch dates was collected from all security bulletins and announcements under all CVE references associated by Secunia with that vulnerability. The start date for a vulnerability is considered to be the date of the earliest announcement, whether from a third-party source or from the operating system vendor. The patch date for a vulnerability is considered to be the date of the latest patch announced in vendor bulletins under all CVE

---

<sup>1</sup> Secunia website, [http://corporate.secunia.com/about\\_secunia/27/about\\_secunia\\_mission/](http://corporate.secunia.com/about_secunia/27/about_secunia_mission/), as accessed on January 2, 2007.

<sup>2</sup> Secunia, personal communication, Michael Hansen, 1/3/07.

---

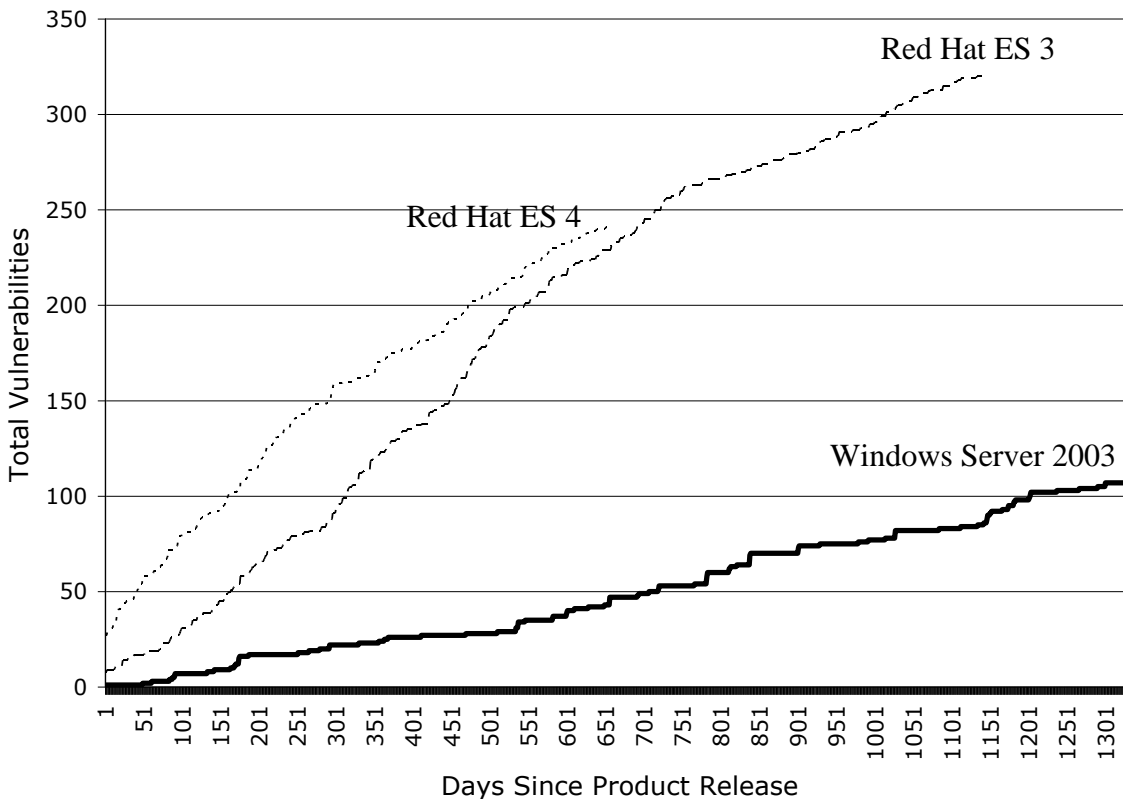
---

references associated by Secunia with that vulnerability. The latest patch date was used because closing a vulnerability may require multiple patches.

### ***Total Vulnerabilities***

The total number of vulnerabilities is one measure of the security of an operating system. In Figure 1 this metric is plotted over the product lifecycle for each operating system. Figure 1 shows Windows Server 2003 is released with fewer initial vulnerabilities than either Red Hat ES 3 or Red Hat ES 4, and has many fewer total vulnerabilities throughout the product lifecycle. Upon release, one vulnerability was identified for Windows Server 2003, compared to 27 for Red Hat ES 4 and eight for Red Hat ES 3. The higher number of vulnerabilities at release for Red Hat ES 3 and 4 is likely explained by their being open-source products, which allows more people to search for and identify vulnerabilities prior to release. At the time of this analysis, Windows Server 2003 had 110 identified vulnerabilities, Red Hat ES 4 had 241, and Red Hat ES 3 had 320. Windows Server 2003 has been in release for 1337 days, Red Hat ES 4 has been in release for 670 days, and Red Hat ES 3 has been in release for 1167 days. Windows Server 2003 has less than half the vulnerabilities either version of Red Hat has despite being in release twice as long as Red Hat ES 4 and six months longer than Red Hat ES 3.

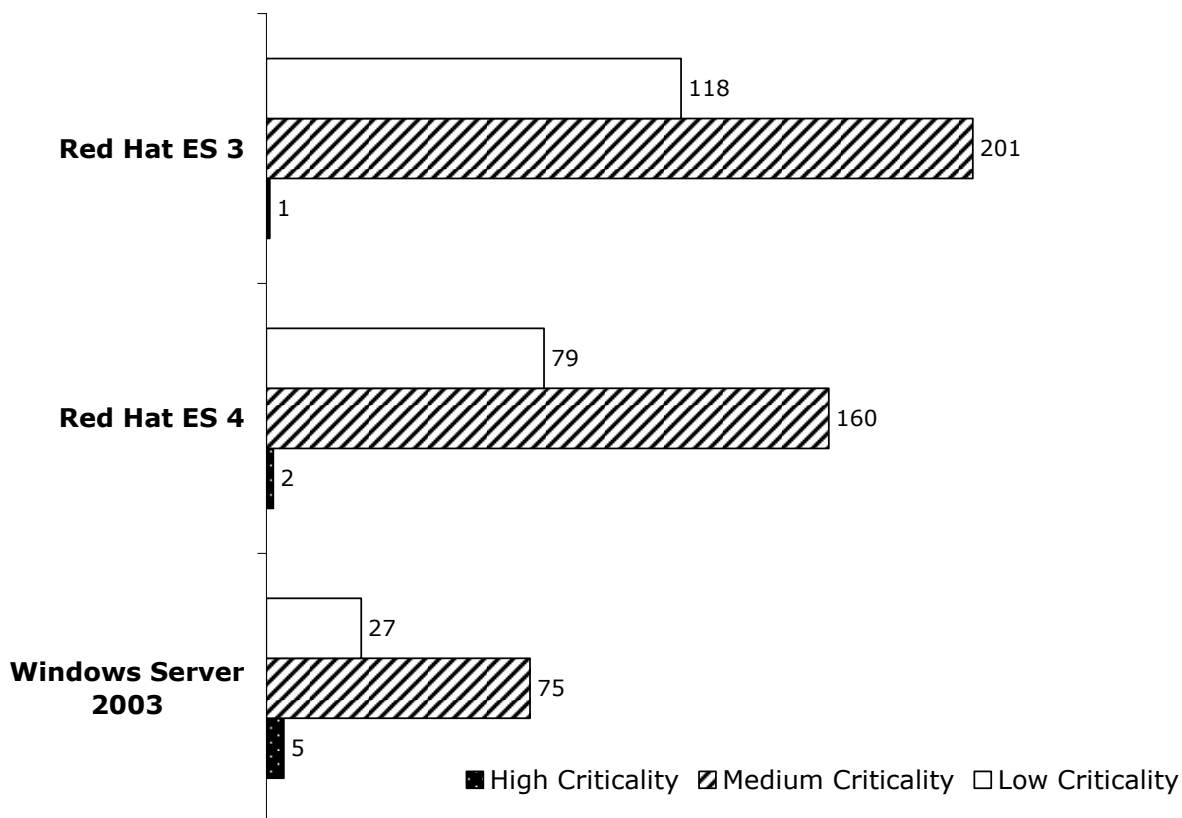
**Figure 1. Total Vulnerabilities for Windows Server 2003, Red Hat ES 3 and Red Hat ES 4**



Each vulnerability represents a different amount of risk; so, to get a sense of the risk, for these three operating systems, the number of vulnerabilities by degree of criticality was also compared. Secunia classifies the criticality of all vulnerabilities on a scale from 1 to 5, with 5 being the most critical. In this analysis, levels 1 and 2 were considered “low” criticality, level 3 and 4 were considered “medium” criticality, and level 5 was considered “high” criticality. Figure 2 shows the number of vulnerabilities by degree of criticality for each operating system. Windows Server 2003 has 1/4 to 1/3 the number of low criticality vulnerabilities as Red Hat ES 3 and Red Hat ES 4, respectively, and less than half the number of medium criticality vulnerabilities. All operating systems have a very low number of high criticality vulnerabilities,

but differ widely in the time after product release it takes to discover the first high criticality. Identifying the first high criticality vulnerability took 45 days for Red Hat 3, 206 days for Red Hat 4, and 811 days for Windows Server 2003.

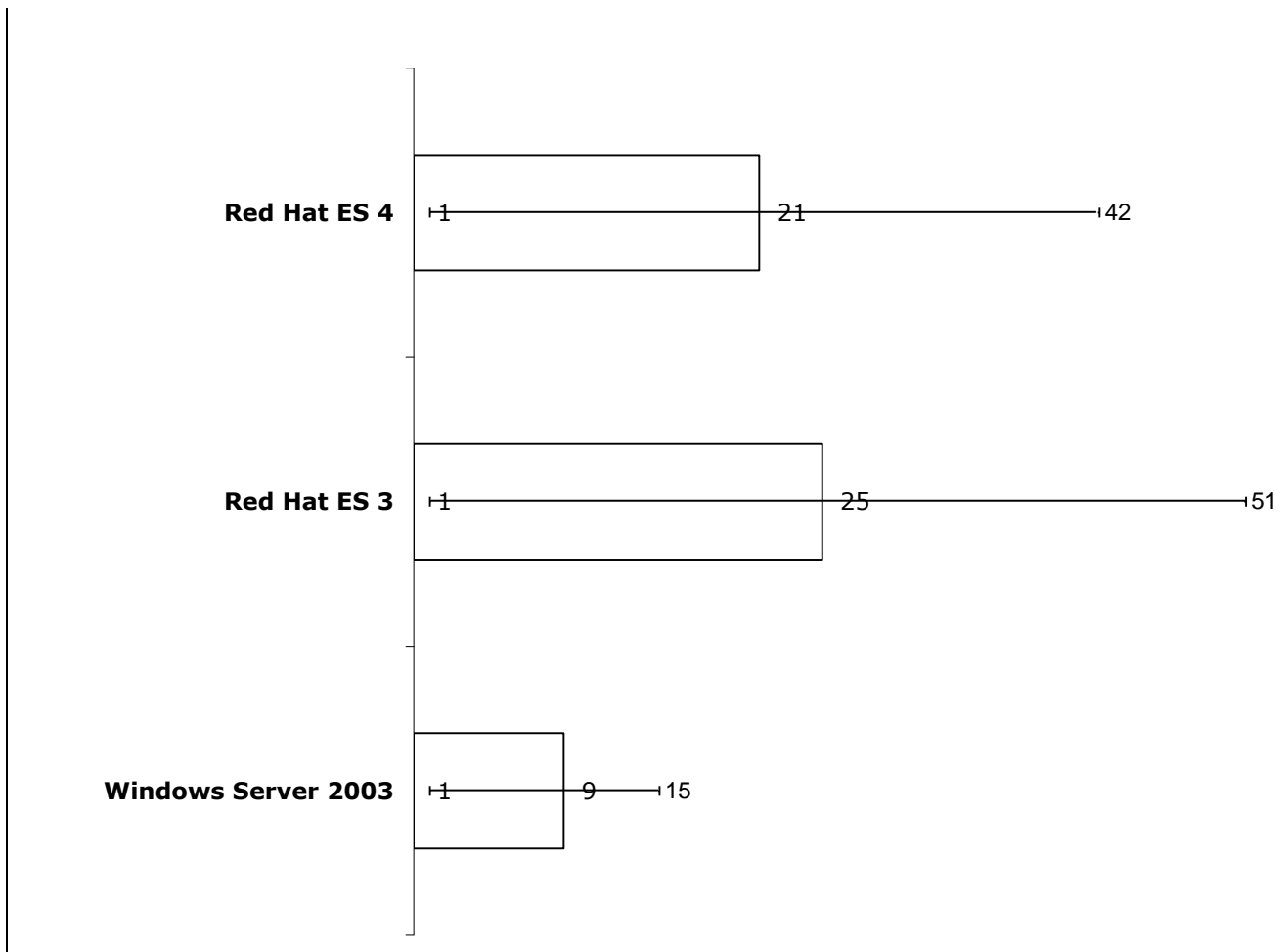
**Figure 2. Total Vulnerabilities by Criticality Level**



### *Unpatched Vulnerabilities*

The average number of unpatched vulnerabilities gives a measure of the daily risk associated with using each operating system. For each operating system, Figure 3 plots the daily average number of unpatched vulnerabilities along with error bars. It shows that on average Red Hat has twice as many unpatched vulnerabilities, and the peak number of unpatched vulnerabilities can be three times higher for Red Hat than for Windows.

**Figure 3. Daily Average Number of Unpatched Vulnerabilities**



## II Conclusions

In summary, Windows Server 2003 is consistently lower risk than Red Hat ES 3 or Red Hat ES 4. Windows Server 2003 has fewer total vulnerabilities, which means users have fewer patching events to respond to, the first high criticality vulnerability was not identified until over two years after release, and on average Windows Server 2003 has fewer unpatched vulnerabilities per day.

---

---

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2007 Microsoft Corporation. All rights reserved.

Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.