

## Sun Operating Systems Also Vulnerable to Security Attacks

John Pescatore

A major vulnerability in a common configuration of two Sun Microsystems operating systems — and the appearance of "exploit code" — shows that security weaknesses aren't just a Microsoft problem.

## NEWS ANALYSIS

---

### Event

On 16 September 2003, iDefense, an Internet security service, announced that it had discovered a major security vulnerability in Sun's Solaris and Trusted Solaris operating systems. A weak set of administration tools — the sadmind(1M) Daemon, which is enabled by default — allows an attacker using a forged identity to take complete control of a Solaris or Trusted Solaris system over port 111. Sun has not offered a patch but has published a set of corrective configuration measures (see [http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56740&zone\\_32=category%3Asecurity](http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56740&zone_32=category%3Asecurity)). Sun says that the next version of Trusted Solaris will disable the vulnerable service by default.

### Analysis

Security flaws in Microsoft's Windows operating system usually result in the most widespread and damaging malicious-code attacks — and the most negative publicity. But other major software providers continue to acknowledge major vulnerabilities in their products. This vulnerability in Sun's operating systems confirms that security weaknesses are by no means limited to Windows.

This flaw rates as High Risk according to the Gartner Internet Risk Vulnerability Ranking method — mainly because exploit code for the flaw has already appeared on the Internet. We have not yet seen increased scanning on the vulnerable port that would signal an imminent attack; nonetheless, we believe an attack is highly likely.

If you use Solaris or Trusted Solaris, *immediately*:

- Block all Internet connections on port 111 at the enterprise firewall
- Take the corrective measures detailed by Sun, which include disabling the vulnerable sadmind(1M) Daemon

This flaw in Solaris and Trusted Solaris also reinforces the importance of a key piece of Gartner advice: Consider the cost of patching and working around security vulnerabilities as a key criterion when you choose operating systems.

**Analytical Source:** John Pescatore, Gartner Research

Written by Terry Allan Hicks, Gartner News

### Recommended Reading and Related Research

- "Internet Vulnerability Risk Rating Methodology" — A simple method lets you classify and prioritize security vulnerabilities. **By John Pescatore**
- "Taxonomy of Software Vulnerabilities" — Different types of software flaws require different detection, assessment and mitigation approaches. **By John Pescatore**

(You may need to sign in or be a Gartner client to access all of this content.)

## REGIONAL HEADQUARTERS

---

Corporate Headquarters  
56 Top Gallant Road  
Stamford, CT 06902-7700  
U.S.A.  
+1 203 964 0096

European Headquarters  
Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

Asia/Pacific Headquarters  
Level 7, 40 Miller Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

Latin America Headquarters  
Av. das Nações Unidas 12.551  
9 andar—WTC  
04578-903 São Paulo SP  
BRAZIL  
+55 11 3443 1509