

# **Are Some RISC-Based Clusters More Secure Than Others?**

**A Detailed Comparison of Potential Vulnerabilities and  
Security-Related Cluster Crashes for HP OpenVMS,  
IBM AIX and Sun Solaris Server Clusters.**



**June 2004  
V1.0**

# Are Some RISC-Based Clusters More Secure Than Others?

## Executive Summary

In February 2004, TechWise Research published a paper entitled: *Total Cost of Ownership for Entry-Level and Mid-Range Clusters*. That paper showed that HP OpenVMS/AlphaServer clusters average fewer hours of security-related downtime than IBM AIX/pSeries and Sun Solaris/Sun Fire clusters. TechWise Research decided to conduct a follow-up study to probe specifically into the area of cluster security. The purpose was to better understand the differences between HP, IBM and Sun cluster security costs, and the possible reasons why HP has an advantage over IBM and Sun in this area. The results from this follow-up research are summarized in this paper.

For this study, TechWise collected and/or analyzed data from four sources. First, availability data from the February 2004 study were examined in more detail, specifically in the area of crashes caused by security-related incidents. Second, we conducted follow-up executive telephone interviews with respondents from the February 2004 study. These in-depth discussions provided further insight into information regarding security issues and availability differences between the three types of clusters. Quotes and comments from respondents are included in this paper. Third, TechWise Research performed a detailed analysis of the CERT® Coordination Center's database that tracks security vulnerabilities and threats. TechWise Research reviewed all the alerts that were issued between January 1, 2000 and December 31, 2003 to identify the number of security patches that have been released for HP OpenVMS, IBM AIX and Sun Solaris. Lastly, TechWise Research studied the Common Vulnerabilities and Exposures (CVE) database that was developed by the MITRE Corporation. This database was started in 1999 to provide standardized names and descriptions for information security vulnerabilities and exposures.

## Overall Results:

The findings show that HP OpenVMS clusters average the fewest hours of security-related downtime, followed by Sun Solaris, and then by IBM AIX clusters which had the most. The difference between the cluster brands is significant. Sun and IBM clusters average three and five hours more of additional security-related downtime per year, respectively, compared to HP clusters. For many companies, the cost per hour of downtime is measured in the tens, if not hundreds of thousands of dollars. Over a three-year period, **HP OpenVMS/AlphaServer clusters have the potential to save companies up to one million dollars, just in security costs, compared to Sun Solaris/Sun Fire and IBM AIX/pSeries clusters.** These savings do not take into account any costs suffered when hackers corrupt or steal confidential information.

TechWise Research identified several reasons why HP OpenVMS/AlphaServer clusters offer the lowest Total Cost of Security™ (TCS™):

- First, Solaris and AIX contain a considerable amount of open source code that is widely available for hackers to access and exploit.
- Second, between Jan. 1, 2000 and December 31, 2003, HP clusters required far fewer security *patches* than IBM and Sun clusters. An examination of the CERT® Coordination Center database revealed only 2 security-related patches for OpenVMS compared with 29 each for AIX and Solaris.
- Third, the OpenVMS operating system has far fewer security *vulnerabilities* than the other two operating systems. A query of the MITRE Corporation's CVE database showed only 5 security vulnerabilities listed for OpenVMS, compared with 89 for AIX and 157 for Solaris.

## Background on This Paper


**Are Some RISC Clusters  
More Secure Than Others?**

**A Detailed Comparison of  
Potential Vulnerabilities  
and Security-Related  
Cluster Crashes for Three  
Different RISC-Based  
Platforms.**

**HP OpenVMS**

**IBM AIX**

**Sun Solaris**

 Cluster Security White Paper, 2004  
© 2004, TechWise Research, Inc.  
Published with permission from TechWise Research, Inc.  
Unauthorized use is strictly prohibited.

1

Application availability has always been an important topic for both server customers and manufacturers alike. In fact, the need for companies to ensure that their primary applications are up and running twenty-four hours a day, 365 days a year, has been a primary catalyst in the adoption of server clusters. Numerous studies, by both TechWise Research and other companies, have shown that the cost of server downtime is considerable and continues to grow. Two factors that can cause significant cluster downtime include computer security breaches and viruses.

Computer security has been an important issue for IT managers for many years. However, in the past few years especially, computer security has come to the forefront and has taken on a whole new level of importance. For many companies, the issue of data security and application availability has expanded beyond the realm of IT managers to now include Executives in corporate boardrooms. Recognizing the importance that their customers place on security and availability, over the past few years, server manufacturers have launched national print and TV advertising campaigns focusing on these very concerns. Why the emphasis on security? First, is the increased number and scope of security/virus events. In 2003, data security was repeatedly front-page news. Major television and Internet news organizations featured articles on security throughout the year. One leading data security company, F-Secure, went as far as to dub 2003 as "The Year of the Worm." This is because of the impact of several high-profile viruses including the e-mail Slammer network worm, Bugbear.B worm, and the Blaster and Sobig.F network worms. Although these viruses primarily targeted Microsoft Windows systems, they rapidly propagated throughout the Internet causing excessive traffic and system instabilities on all types of servers worldwide. The Sobig.F worm alone resulted in 300 million infected e-mail messages worldwide.

Second, new security threats continue to develop and emerge. As of the writing of this report, several high-impact security threats are being tracked by the industry including the W32/Korgo.F worm, the W32/Sasser worm, and the Phatbot Trojan. Clearly the threat of viruses and worms will continue to plague IT managers for the foreseeable future.

Terrorism is another reason for the invigorated focus on computer security. The threat of cyber-attacks looms ever more likely, especially in the wake of 9-11. The U.S. Federal Government recognizes this vulnerability to cyber-attacks and understands its potential impact. As such, the U.S. Department of Homeland Security now funds several non-profit organizations. These organizations alert businesses and the general public about current security threats, as well as provide steps companies and individuals can take to protect their computer systems from becoming infected. TechWise analyzed security-related data from two of these organizations (CERT® Coordination Center and the MITRE Corporation) and incorporated the results into this research paper.

The text slide on the right provides excerpts from a speech given by Tom Ridge, U.S. Secretary of Homeland Security, at the 2003 National Cyber Security Summit. In his talk, *Secretary Ridge points out that there were more than 76,000 cyber security incidents in the first six months of 2003.* He also points out the importance of our protecting our cyber assets.

In February 2004, TechWise Research published a paper entitled: *Total Cost of Ownership for Entry-Level and Mid-Range Clusters.* That paper provided details

regarding the Reliability-Adjusted Total Cost of Ownership™ of various RISC-based server clusters<sup>1</sup>. Part of the analysis in that paper showed that HP OpenVMS/AlphaServer clusters experienced less downtime due to viruses and worms than similar IBM AIX/pSeries and Sun Solaris/Sun Fire clusters. TechWise Research decided to conduct a follow-up study to probe into the area of security in greater detail. This paper summarizes our findings. We provide a more robust study of the differences between HP, IBM and Sun cluster security costs, and explore possible reasons why HP has an advantage over IBM and Sun in this area.

**Remarks by Tom Ridge**  
**U.S. Secretary of Homeland Security**  
**National Cyber Security Summit - December 3, 2003**

*"The sheer reality is that we rely on computers. In many visible ways, the applications of computing are a part of our everyday life...e-mail, Internet research, online shopping. However there are countless other ways computers impact us daily that as a society we take for granted..."*


*A vast electronic nervous system operates much of our nation's physical infrastructure. Everything from electricity grids to banking transactions to telecommunications depends on secure, reliable cyber networks...*

*These networks and the infrastructures they support present an attractive target for terrorists. They know, as do we, that a few lines of code could ultimately wreak as much havoc as a handful of bombs...*

*And the unfortunate truth is that the number of cyber-security incidents is on the rise. More than 76,000 occurred in just the first six months of [2003]...*

*For every hacker or terrorist that tries to throw a worm or virus in our way, we must have effective roadblocks and tough barricades to throw in theirs..."*

- Tom Ridge, Secretary, U.S. Department of Homeland Security, December 2003



Cluster Security White Paper, 2004  
 © 2004, TechWise Research, Inc.  
 Published with permission from TechWise Research, Inc.  
 Unauthorized use is strictly prohibited.

2


## Who Was Surveyed

**Two-Phase Methodology**

- **Phase 1:** A total of 94 web-based surveys were completed with U.S.-based IT professionals in the Fall of 2003.
  - All respondents were pre-screened to ensure they had a qualifying cluster and that the cluster was installed for at least six months.

Brand	Completed Surveys
HP AlphaServer OpenVMS	32
IBM RS/6000 or pSeries AIX	32
Sun Enterprise or Sun Fire Solaris	30

- **Phase 2:** Follow-up executive phone interviews were completed in the Spring of 2004.



Cluster Security White Paper, 2004  
 © 2004, TechWise Research, Inc.  
 Published with permission from TechWise Research, Inc.  
 Unauthorized use is strictly prohibited.

3

This follow-up research study on security costs is based on the 94 web-based interviews that TechWise completed with IT professionals in the Fall of 2003. The chart to the left summarizes the participants in the original "Phase 1" study, as well as the approach and purpose for this current follow-up study ("Phase 2").

The Phase 1 "quantitative" survey was designed to collect operational and profiling data about the cluster itself, as well as demographic information about the company using it. Throughout that web survey, respondents were given

several opportunities to clarify any answers they provided. One of TechWise Research's senior analysts, who specializes in server clusters, personally reviewed each completed survey and followed-up with respondents by phone if any answers needed clarification.

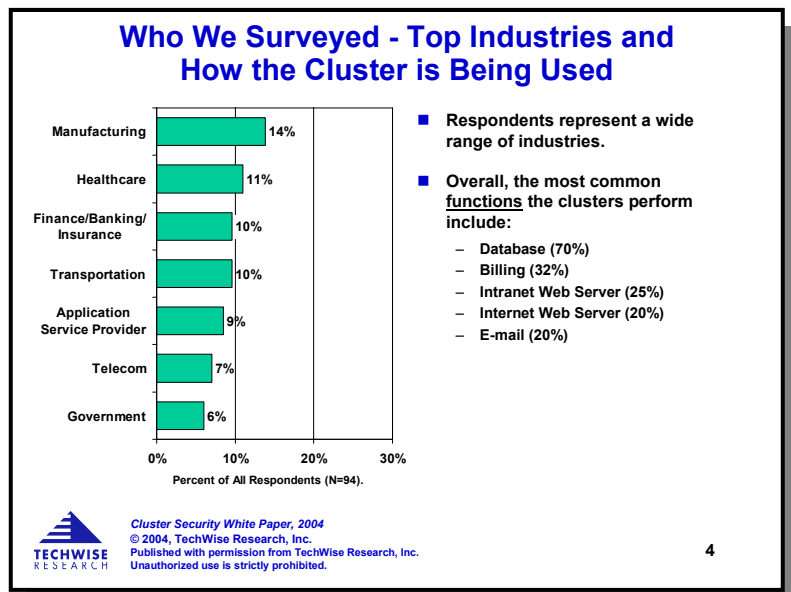
To qualify for the web-study, all respondents were carefully screened to ensure that they personally managed a qualifying entry-level or mid-range cluster. Furthermore, all clusters were required to meet the following four screening criteria:

1. The cluster was one of three target server platforms: HP AlphaServer running OpenVMS, IBM RS/6000 or pSeries running AIX, or Sun Enterprise or Sun Fire servers running Solaris. (Note: For the remainder of this paper, the IBM platform will be referred to as the "pSeries," and the Sun platform as "Sun Fire.")
2. The cluster used the manufacturer's clustering software. Therefore, all HP clusters use OpenVMS Cluster, all IBM clusters use HACMP, and all Sun clusters use Sun Cluster. Clusters that were using third-party clustering software, such as Veritas, were excluded from the analysis.
3. The cluster did not contain any enterprise-class servers. An enterprise-class server was defined as one that supports more than 16 processors.
  - Examples of disqualifying systems for HP include the AlphaServer GS 320 and GS 1280 M32 and M64. For IBM, the p680, p690, and RS/6000 S80 did not qualify. For Sun, any cluster that contained Ultra Enterprise 6000, Enterprise 6500 or 10000, Sun Fire 6800, 12K or 15K servers, was disqualified for this study.
4. The cluster was running in a *production mode* for at least six months. Clusters used in development and/or testing, or for less than 6 months, were excluded from the study.

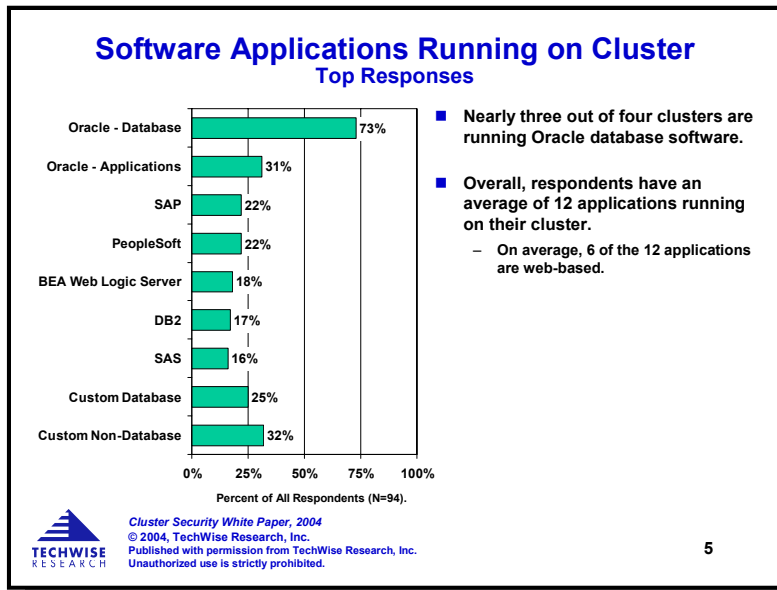
To gain insights into the security results from Phase 1, TechWise Research conducted follow-up executive phone interviews with some of the Phase 1 respondents. Each interview lasted approximately 45 minutes and was personally conducted by the president of TechWise Research. The interviews were conducted with senior IT respondents from the following companies: (1) a software company that develops information systems for hospitals and medical clinics, (2) a global financial services company that has nearly \$4 trillion in assets under management/administration/custody, (3) one of the largest banks in the U.S., (4) a leading insurance company that has 50 million customers, (5) a leading information service company whose website receives nearly 2 million visitors each month who purchase information online, (6) one of the largest U.S. wireless communications companies, (7) a transportation company that maintains a fleet of aircraft that it leases to a major international airlines, and, (8) a robotics company that develops manufacturing solutions for the automotive industry.

## Company & Respondent Profile

All participants were randomly recruited from a broad mix of industries, as shown in the chart to the right. The top represented industries in the study include: manufacturing, healthcare, finance/banking/insurance, & transportation. Most of the study's respondents work for large companies. Twenty-six percent work for companies with 10,000 or more employees worldwide, 15% have between 5,000 - 9,999 employees, and 34% work for companies with 1,000 - 4,999 employees worldwide. In terms of function, two out of three



reported that their cluster is being used to perform a database function. Between 1/5 and 1/3 of the clusters were performing billing, web server and e-mail functions.

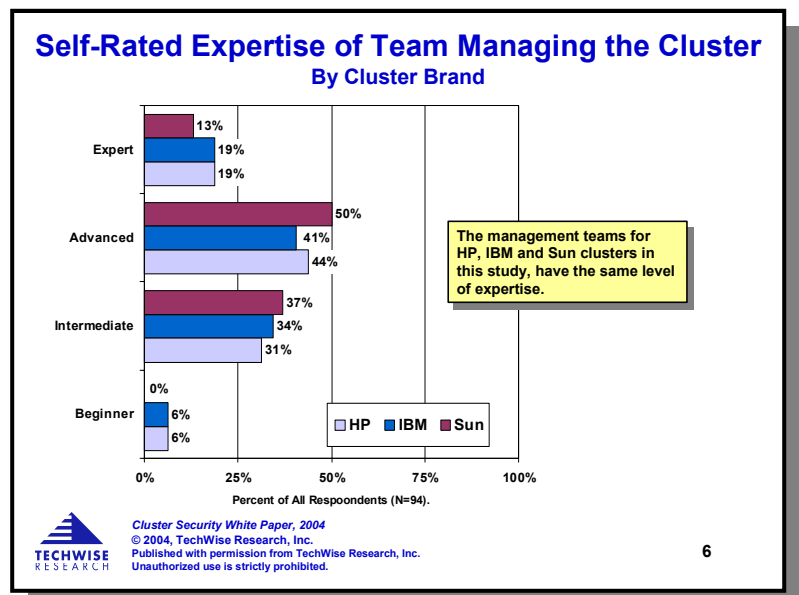


The chart to the left illustrates the top software applications running on the clusters. The majority of the clusters in this study are running one or more database applications. Nearly three out of four have an Oracle database. In terms of the number of end-user applications, the clusters are running an average of 6 web-based and 6 non-web-based applications. IBM clusters averaged the most number of web-based applications (8) compared with HP that averaged the fewest (4). Despite these differences in the number of web-based applications, HP OpenVMS/AlphaServer clusters had the highest average number of end-users accessing the cluster's web-based applications. In a typical 24-hour period, HP clusters averaged 3,600 end-users, versus 2,900 for IBM and 1,800 for Sun.

had the highest average number of end-users accessing the cluster's web-based applications. In a typical 24-hour period, HP clusters averaged 3,600 end-users, versus 2,900 for IBM and 1,800 for Sun.

In terms of experience, the teams managing the clusters in the study are well-practiced, competent users of their particular cluster brand. Overall, 62% of respondents rate the skill level of the team managing the cluster as either "advanced" or "expert." Only 4% rate their team at a "beginner" level. As shown in the chart to the right, expertise did not statistically vary by cluster brand.

Additionally, for the companies that in part, or in whole, manage their clusters on site (which is the majority of firms surveyed), have been working with their respective cluster brand software for an average of 4 years



The management teams for HP, IBM and Sun clusters in this study, have the same level of expertise.



## Reasons Why IT Managers Are More Concerned About Security Today

### Respondent Comments About the Importance of Security

*"Viruses and worms are much more of a threat now than they were 18 months ago. We have assigned someone to focus on this full-time."*

*"We formed a team that meets once a month to discuss our security strategy."*

*"We set up a dedicated team 12 months ago to focus on viruses, worms and other security threats."*

*"Cost used to be the number one factor we considered when evaluating new servers. Now it is number two or three behind security."*



Cluster Security White Paper, 2004  
© 2004, TechWise Research, Inc.  
Published with permission from TechWise Research, Inc.  
Unauthorized use is strictly prohibited.

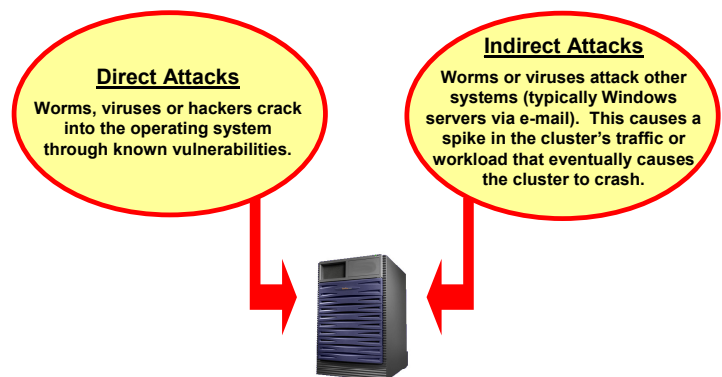
7

IT managers have long been concerned with the issue of network and data security. After reviewing respondent comments from the Phase 1 "quantitative" survey, and after speaking with IT managers at length in the Phase 2 "qualitative" interviews, it became clear that their level of concern has escalated. When asked to describe the importance of security, several common themes emerged. First, is that threats today are more sophisticated. Viruses and worms are more robust and harder to identify because hacker code is less overt, and is functioning in a more

"stealthy" manner. This makes it increasingly difficult for IT managers and security experts to identify and intercept a new threat before it has spread and/or propagated. The second theme is that the code itself is more insidious and damaging. It used to be the thrill of breaking into a site, and subsequent bragging rights, that motivated many hackers. Today, however, this is changing. Hackers are more frequently being employed and deployed as instruments of destruction for those with economic, political, social, and religious agendas. The threat, therefore, is much greater. It is not surprising then that most of the respondents we interviewed indicated that their company's investment level in security products and services has increased over the past 18 months. IT staff, and in some cases entire teams, have been dedicated to the issue of security. One respondent went as far as to say that security is now the number one issue they consider when evaluating new platforms, even ahead of price.

A number of the high-profile security threats over the past few years specifically targeted systems running Microsoft Windows. This current study, however, focuses on RISC-based server clusters. One goal of the Phase 2 interviews was to understand if and how malicious code that targets Microsoft machines impacts RISC-based server clusters. Summarizing their answer to this question, respondents explained that their systems face both "direct" and "indirect" security threats. These are described in the chart to the right. The first type of threat, a direct threat, is malicious code that is specifically designed to attack their cluster's specific operating system. This type of attack would attempt to take advantage of vulnerabilities in AIX, OpenVMS, Solaris or UNIX operating systems.

### Two Types of Security Threats Clusters Face

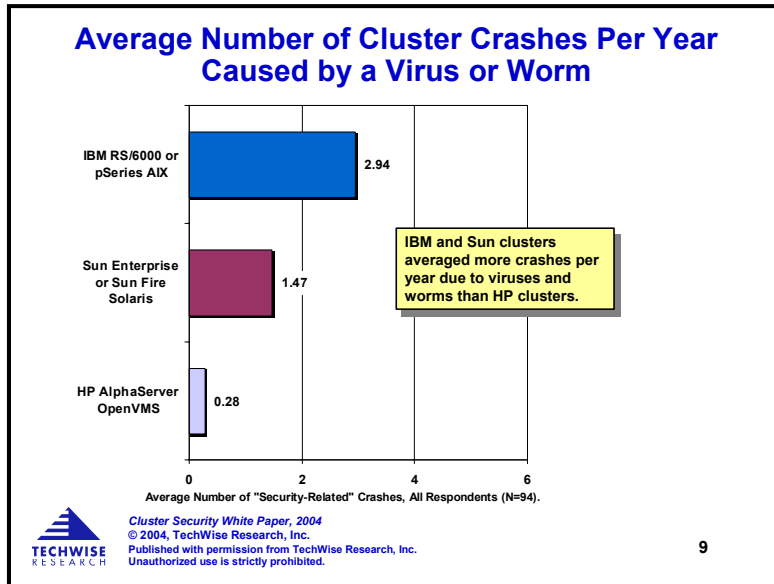


Cluster Security White Paper, 2004  
© 2004, TechWise Research, Inc.  
Published with permission from TechWise Research, Inc.  
Unauthorized use is strictly prohibited.

8

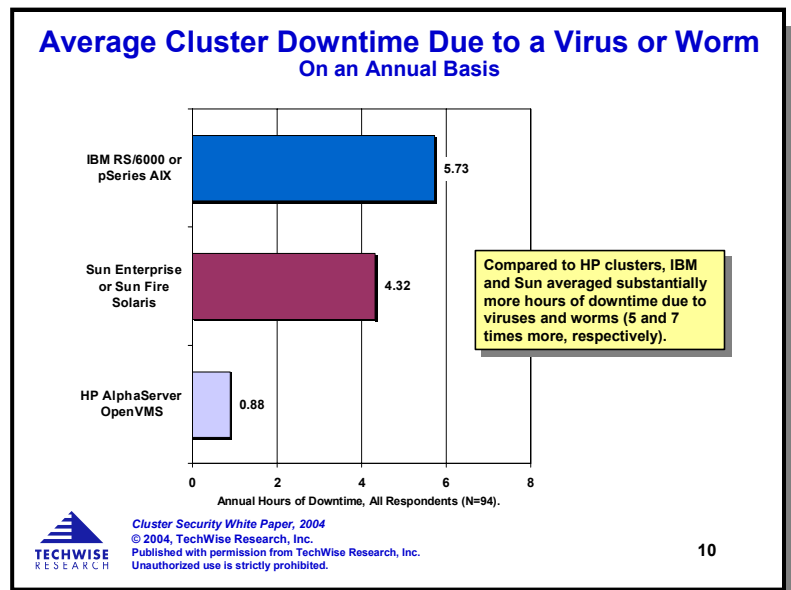
The second type of threat is an indirect threat. This is where a worm or virus is designed to attack a different type of system, typically a Microsoft Windows web or e-mail server. Although the RISC-based cluster is not specifically targeted, it is not immune to the affects of an indirect attack. This is because many RISC-based clusters communicate with Windows servers either behind their corporate firewall and/or over the Internet. Once the Windows server is infected, it has the potential to impact a RISC-based cluster by creating huge spikes in traffic and cluster workload. This domino effect can cause the cluster to slow down, become sluggish and eventually crash.

## How Often RISC-Based Clusters Crash Due to a Virus or Worm



In the quantitative survey, a cluster crash was defined as any event that caused the cluster's primary application(s) to become unavailable to end-users (i.e., go offline). In that survey, respondents indicated how many times, if any, their cluster crashed specifically due to a virus or worm. The chart to the left summarizes the findings. Overall, respondents using IBM AIX clusters experienced the highest number of security-related cluster crashes per year, followed by Sun Solaris clusters. HP OpenVMS clusters averaged the fewest number of security-related cluster crashes.

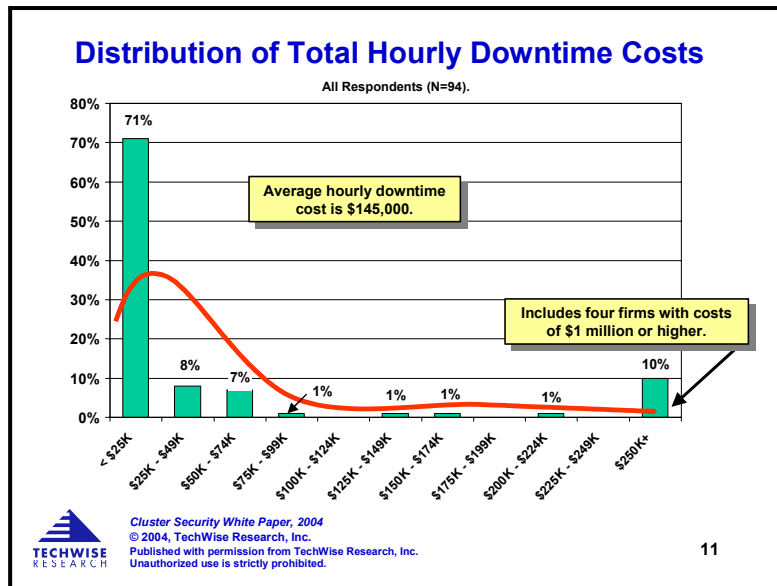
There are two components to measuring cluster availability. First, is the number of crashes experienced. Second, and perhaps more importantly, is how long the cluster was down because of the crash. For this reason, TechWise Research not only collected information about the number of security-related crashes, but also collected information about the actual downtime resulting from these virus and worm-related crashes. The chart below illustrates the average number of hours per year each brand of cluster was offline due to a crash caused by a virus or worm. This chart shows that respondents with IBM clusters averaged 5.73 hours of downtime per year due to viruses or worms. This is compared to 4.32 hours for Sun and only 0.88 hours for HP per year. **Compared to HP OpenVMS clusters, the IBM AIX and Sun Solaris clusters averaged substantially more hours of security-related downtime (5 and 7 times more, respectively).** This difference in availability has the potential to have a major impact on a company's operations, as will be shown in the upcoming sections.





## Quantifying the Impact of Security-Related Cluster Downtime

In the quantitative survey, respondents were asked to rate the importance of nine different factors in future cluster purchase decisions. The two most important factors include: 1) The cluster's overall reliability, and 2) How well the cluster software performs when there is a failure. The other top factor is the security features that are built into the operating system. These importance findings demonstrate the overall value IT Managers place on availability, and further re-enforces the primary reason for establishing a cluster - to ensure that primary applications are available to end-users 24x7. Downtime matters to IT managers.

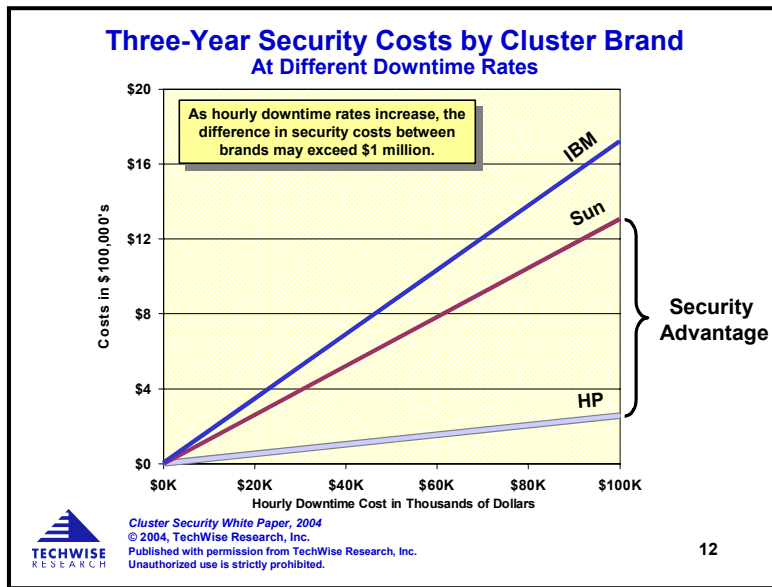


As reported in prior TCO studies conducted by TechWise Research, each company has a unique situation that determines the financial impact of downtime. For some, when primary applications are not available to end-users, the impact is lost sales. For others, it means lost employee productivity or a decline in manufacturing production. Many firms are affected in multiple ways. TechWise Research asked each respondent to quantify the financial impact for each hour of downtime. As shown in the chart to the left, the distribution of downtime costs varies greatly. On average, however,

respondents report that **each hour of downtime costs their firm a total of \$145,000** when the costs associated with lost sales, wages, and production are considered. This represents a 30% increase over the costs reported in TechWise's 2001 low-end (i.e., entry-level) and mid-range cluster TCO paper.

The above downtime cost figures demonstrate the considerable impact availability has on a corporation's bottom line. However, the above costs *likely understate the impact of security-related crashes*. Unlike crashes caused by hardware failures or power outages, many security-related crashes have a malicious component. Hackers and viruses often corrupt data before causing a crash. This may result in additional time and costs to restore that data which is not reflected in the chart above.

## Total Cost of Security Findings



The chart to the left summarizes the Three-Year Total Cost of Security™ (or TCS™) findings for the three cluster brands studied. These costs are projected over a three-year period since previous studies indicate this is an appropriate timeframe for the class of server cluster represented in this research. Since each company has a unique cost associated per hour of downtime, the chart shows how TCS™ varies at different downtime rates.

All three brands are the same when there are no costs associated with

cluster downtime. As downtime costs increase, however, security costs vary considerably between brands. HP OpenVMS AlphaServer clusters have a much lower security cost compared to Sun Solaris/Sun Fire and IBM AIX/pSeries clusters. When an hour of cluster downtime results in a cost of \$20,000, HP's advantage over Sun and IBM is \$206,000 and \$291,000, respectively, over a three-year period. When an hour of downtime costs a company \$100,000, HP's advantage grows to \$1 million and \$1.46 million compared to Sun and IBM over a three-year period. **In summary, when the costs of security-related cluster crashes are projected over a three-year period, HP OpenVMS/AlphaServer clusters have the potential to save companies up to a million dollars or more compared to comparable Sun Solaris/Sun Fire and IBM AIX/pSeries clusters.**

## Respondents' Opinions on Differences in Operating System Security

As part of the qualitative interviews, respondents were asked to provide their perceptions regarding the similarities and differences between AIX, Solaris and OpenVMS on the issue of security. Several respondents have experience with two or more of these operating systems and could make direct comparisons. Others restricted their comments to the operating system running on their cluster. A few interesting findings came out of these discussions. First, several respondents commented that all flavors of UNIX have security vulnerabilities because they use open source code. One IT Manager provided the following opinion on this subject: "UNIX is a good operating system, but is open and is vulnerable to hacking. All the flavors of UNIX use portions of open source code that hackers have access to." Several respondents made comments that support this statement. They also pointed out the

**Respondent Comments About Differences in Operating Systems' Security Vulnerabilities**

"UNIX is a good operating system, but it is open and is vulnerable to hacking. All the flavors of UNIX use portions of open source code that hackers have access to."

"Unfortunately, we have to constantly apply patches to our UNIX and Windows servers to make sure we are as safe as possible."

"The Sun servers seem to be more vulnerable to viruses than some others I have worked with previously. But maybe they crash more often because they are overloaded."

"If you do not keep your IBM cluster updated, you will run into security problems."

"IBM sends us a set of CD's roughly once a month with security information, updates and patches. I like the fact that the CD is customized for the IBM systems I have."

"OpenVMS is a pretty secure system. I can only recall two patches being released over the past few years - and one did not apply to us based on how we use our cluster."

"OpenVMS is definitely more secure. Less exploits are written for it. A single UNIX exploit could be tweaked to work across multiple UNIX variants."

TECHWISE RESEARCH  
Cluster Security White Paper, 2004  
© 2004, TechWise Research, Inc.  
Published with permission from TechWise Research, Inc.  
Unauthorized use is strictly prohibited.

13

need to frequently apply security patches to AIX or Solaris. Interestingly, this was not always viewed as a negative. One respondent with an IBM cluster lauded IBM's efforts to provide him with patch CDs that are customized for his exact system and configuration. Another Sun respondent commented that the fact that "Sun releases so many security patches tells me that they are keeping up with new threats and care about the security of my system." One IBM respondent, who is familiar with both AIX and OpenVMS, commented that "OpenVMS is robust and very stable where AIX has had more patches and updates."





It is interesting that the HP OpenVMS respondents have a different perspective on patches and vulnerabilities compared to the IBM AIX and Sun Solaris respondents. All of the OpenVMS respondents interviewed commented that the operating system is secure and stable. They point out that OpenVMS has had very few security patches over the past few years, and that it does not suffer the same vulnerabilities as UNIX. IBM and Sun respondents, on the other hand, almost seem re-assured that there are many patches and updates, even if it creates more work.

Based on the interview discussions, it appears that one reason HP OpenVMS clusters have fewer security-related cluster crashes is because the operating system is more stable and secure. This hypothesis, however, is based on a relatively small number of qualitative interviews. TechWise Research, therefore, decided to conduct a robust search for secondary information to test the validity of this hypothesis. The results of this search are summarized in the next report section.

## Independent Evaluations of Operating System Security

### Sources Used to Analyze Security Threats

- **CERT/CC**
  - The CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.
  - Website: [www.cert.org](http://www.cert.org)
- **Common Vulnerabilities & Exposures**
  - CVE is a list of common names for publicly known information security vulnerabilities and exposures. It is maintained by the MITRE Corporation, an independent, not-for-profit corporation.
  - Website: [www.cve.mitre.org](http://www.cve.mitre.org)
- **U.S. Department of Homeland Security**
  - Funds both CERT/CC and CVE.
  - Website: [www.us-cert.gov](http://www.us-cert.gov)



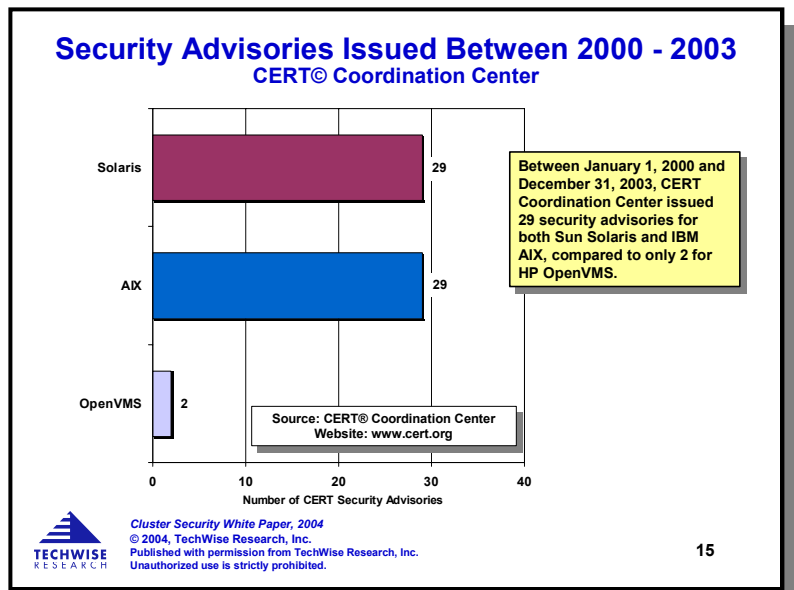
Cluster Security White Paper, 2004  
© 2004, TechWise Research, Inc.  
Published with permission from TechWise Research, Inc.  
Unauthorized use is strictly prohibited.

14

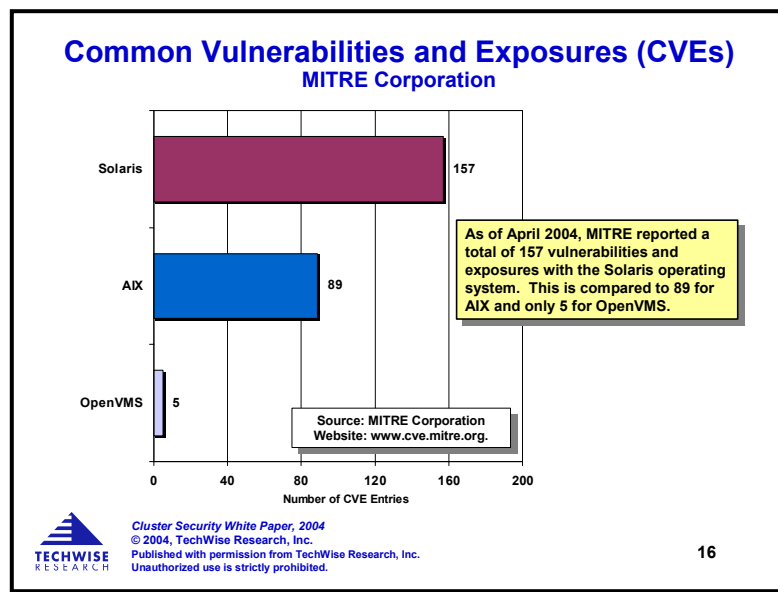
TechWise Research identified two organizations that track security issues for various computer platforms. A description of these organizations, along with their website addresses, are shown in the text slide to the left. The CERT® Coordination Center (CERT/CC) is a major reporting center for Internet security problems. Run by Carnegie Mellon University and primarily funded by the U.S. Department of Defense and the Department of Homeland Security, CERT/CC is a center of Internet security expertise. CERT/CC staff members analyze product vulnerabilities, provide

technical advice, and coordinate responses to security compromises. The second information source is the Common Vulnerabilities and Exposures (CVE) database that is maintained by the MITRE Corporation. This database is a list of common names for publicly known information security vulnerabilities and exposures. TechWise Research analyzed the databases from both organizations in an effort to prove or disprove respondents' hypothesis regarding operating system security.

The CERT/CC website offers a search tool that allows users to conduct a keyword search for advisories. This tool could be used to quickly get a count of all advisories that list AIX, OpenVMS and/or Solaris. This approach, however, would yield misleading results. This is because the CERT/CC advisories are very detailed. They often list responses from a number of manufacturers as to whether or not their products are vulnerable to the particular identified threat. A simple search will yield many false positives, since operating systems that are listed as immune to a threat would come up as a positive hit. To avoid this issue and derive a more accurate measure of each operating systems' vulnerabilities, TechWise Research conduct a thorough analysis of the CERT/CC database. This analysis included a review of every advisory that was issued between January 1, 2000 and December 31, 2003, to determine which ones required a security patch to be installed on Solaris, AIX or OpenVMS. The results of this analysis are illustrated in the chart to the right. **During this three-year period, Sun and IBM each released a total of 29 patches in response to security vulnerabilities identified by CERT/CC. During this same period, a total of 2 patches were released for OpenVMS.**



The above chart provides independent, quantifiable proof that Sun Solaris and IBM AIX require many times more security patches than HP OpenVMS. TechWise Research does recognize that some vulnerabilities will only apply to a subset of clusters that are using a particular routine or configuration. Therefore, to help readers identify how many patches apply to their systems, we included an Appendix in this paper that lists all of the vulnerabilities identified in our analysis of the CERT database, and which operating systems are affected by them.



The MITRE Corporation is an independent, not-for-profit company that provides technical support to the U.S. Government on information security issues. In 1999 MITRE started the Common Vulnerabilities and Exposures (CVE) initiative, a publicly available "dictionary" that provides standardized names and descriptions for information security vulnerabilities and exposures. MITRE creates the CVE list in cooperation with 35 major security organizations that comprise the CVE Editorial Board, including CERT Coordination Center, IBM, Internet Security Systems (ISS), National Security Agency (NSA), the SANS (SysAdmin, Audit, Network, Security) Institute, and Sun Microsystems.

TechWise Research queried the CVE database in April 2004 to determine how many security vulnerabilities have been identified for Solaris, AIX and OpenVMS. The results of this query are illustrated in the chart on the previous page. The Solaris operating system had the greatest number of CVE listings with a total of 157. IBM's AIX had roughly half of Sun's total with 89, while HP's OpenVMS only had 5 listings. **According to the CVE database, the Solaris and AIX operating systems have 31 times and 18 times, more security vulnerabilities, respectively, than OpenVMS.**

These two independent sources, therefore, support several of the comments made by respondents in the qualitative interview phase of this study.

- First, the table in the Appendix that lists all relevant CERT advisories shows that the two UNIX operating systems, AIX and Solaris, share many of the same vulnerabilities. This supports respondents' comments that these two operating systems have many of the same vulnerabilities since they both integrate the same open source code.
- Second, the fact that OpenVMS is immune to all but one of the vulnerabilities of AIX and Solaris, supports respondents' hypothesis that OpenVMS is less vulnerable to security threats.
- Third, the CERT database shows both AIX and Solaris having 29 security advisories issued over the past three years. This supports respondents' comments about the frequency of security patches that they need to apply to these operating systems.
- Lastly, one respondent with experience with both AIX and Solaris commented that AIX appeared to be the more secure of the two operating systems. This hypothesis is supported by the CVE database that shows Solaris as having two times more vulnerabilities than AIX.

## Why OpenVMS is More Secure

Respondents who were managing OpenVMS clusters made a number of comments regarding the security of this environment. Samples of these comments are listed in the text slide to the right. One respondent said that "OpenVMS is difficult to hack," and even if one had permission to access a system as a user, it is still very hard to hack into other areas of the system. In addition to protecting valuable information, there is another benefit of the high level of security offered by OpenVMS. HP OpenVMS clusters are relatively easy to manage. Once installed and configured, they rarely require security-related patches. This

saves IT Managers time and potential headaches. One IBM respondent commented that security patches could be tricky to install: *"The IBM cluster takes some getting used to. Upgrades to the operating system are very difficult. If one small thing is missing, like a DLL, or is done incorrectly, like a system file is setup incorrectly, it is a nightmare to find it. Sometimes these problems are not documented, but our IBM Global Services consultant knows about them."* Additional information on the subject of cluster management is in TechWise Research's recently published paper: *Are some RISC-Based Clusters Easier to Manage Than Others?*<sup>(1)</sup>

### Respondent Comments Regarding the Security of HP OpenVMS/AlphaServer Clusters

*"OpenVMS is hard to hack into. Even if you log in as a user, it is hard to hack into other areas."*

*"OpenVMS has a high rating in security from the U.S. Department of Defense... If someone is worried about security and stability, I highly recommend OpenVMS."*

*"OpenVMS was designed from the ground up as a time sharing operating system. Security was not an afterthought."*

*"I wish all the rest of our IT environment were as reliable as our OpenVMS cluster. It would make my life a lot easier."*



Cluster Security White Paper, 2004  
© 2004, TechWise Research, Inc.  
Published with permission from TechWise Research, Inc.  
Unauthorized use is strictly prohibited.

17



## Conclusion

Computer security has taken on a whole new dimension of economic consequence. The importance of data availability and security is no longer primarily a matter for the IT department or manager to address. Rather, its resolution, scope and strategy extends from Executives in corporate boardrooms to the U.S. Department of Homeland Security. This white paper provided an in-depth analysis of the cluster crashes that are specifically caused by security-related issues such as viruses and worms. It compared the Three-Year Total Cost of Security™ for three brands of RISC-based server clusters: HP OpenVMS/AlphaServer, IBM AIX/pSeries, and Sun Solaris/Sun Fire. Data from TechWise Research's February 2004 TCO study, and subsequent white paper (*Total Cost of Ownership for Entry-Level and Mid-Range Clusters*) were further analyzed, and then combined with results from in-depth respondent interviews, as well as with results from additional research, to provide the findings in this paper.

The findings show that IBM AIX clusters averaged the highest number of security-related downtime hours per year, followed by Sun Solaris, and HP OpenVMS clusters with the least. The difference between cluster brands is significant. IBM AIX clusters averaged 5.73 hours of security-related downtime per year, compared to 4.32 hours for Sun Solaris and only 0.88 hours for HP OpenVMS. **When the costs of security-related cluster crashes are projected over a three-year period, HP OpenVMS/AlphaServer clusters have the potential to save companies up to a million dollars or more compared to comparable IBM AIX/pSeries and Sun Solaris/Sun Fire clusters.**

### Top Reasons Why HP OpenVMS Clusters Have the Lowest Security Costs of the Three Brands

- Solaris and AIX contain open source code that hackers can access. OpenVMS is a closed system that was designed with security in mind.
- Between Jan. 1, 2000 and December 31, 2003, HP clusters required far fewer security patches than IBM and Sun.
  - Only 2 for HP compared with 29 for IBM and 29 for Sun.
    - Source: CERT® Coordination Center.
- OpenVMS has far fewer security vulnerabilities than the other two operating systems.
  - Only 5 for HP compared with 89 for IBM and 157 for Sun.
    - Source: MITRE Corporation.



Cluster Security White Paper, 2004  
© 2004, TechWise Research, Inc.  
Published with permission from TechWise Research, Inc.  
Unauthorized use is strictly prohibited.

18

TechWise Research conducted qualitative interviews with respondents and analyzed two independent data sources to identify the reasons for these differences. **The results of this research support the conclusion that HP OpenVMS clusters are more secure than IBM AIX and Sun Solaris clusters.**

Protecting sensitive information has never been more challenging than it is today. IT Managers face threats on numerous fronts. Many have dedicated individuals or entire teams that focus exclusively on data security. This paper shows that not all operating

systems offer the same level of security. Furthermore, the impact of a security-related crash is considerable. Security, therefore, is an important factor to consider in the purchase decision process.

TechWise Research is an independent primary market research firm that specializes in the computer industry. If you have any questions regarding this research, please contact us at:

[TCS2004@TechWise-Research.com](mailto:TCS2004@TechWise-Research.com)

AlphaServer and OpenVMS are trademarks of Hewlett-Packard. RS/6000 and pSeries are trademarks of IBM. CERT and CERT/CC are trademarks of Carnegie Mellon University. CVE is a trademark of The MITRE Corporation. Total Cost of Security (TCS) is a trademark of TechWise Research, Inc.

(1) For a free copy of any current TechWise Research report, including the papers entitled *Total Cost of Ownership for Entry-Level and Mid-Range Clusters* and *Are Some RISC-Based Clusters Easier to Manage Than Others?* visit: [www.techwise-research.com/whitepapers.html](http://www.techwise-research.com/whitepapers.html)



## Appendix: Summary of CERT/CC Advisories Between January 1, 2000 and December 31, 2003

CERT Advisory	HP OpenVMS	IBM AIX	Sun Solaris
CA-2003-26 Multiple Vulnerabilities in SSL/TLS Implementations	Safe	Vulnerable <sup>(2)</sup>	Safe
CA-2003-25 Buffer Overflow in Sendmail	Safe	Vulnerable	Vulnerable
CA-2003-24 Buffer Management Vulnerability in OpenSSH	Safe	Vulnerable <sup>(2)</sup>	Vulnerable
CA-2003-12 Buffer Overflow in Sendmail	Safe	Vulnerable	Vulnerable
CA-2003-10 Integer overflow in Sun RPC XDR library routines	Safe	Vulnerable	Vulnerable
CA-2003-07 Remote Buffer Overflow in Sendmail	Safe	Vulnerable	Vulnerable
CA-2003-02 Double-Free Bug in CVS Server	Safe	Vulnerable <sup>(2)</sup>	Vulnerable <sup>(3)</sup>
CA-2002-36 Multiple Vulnerabilities in SSH Implementations	Vulnerable	Safe	Safe
CA-2002-34 Buffer Overflow in Solaris X Window Font Service	Safe	Vulnerable	Vulnerable
CA-2002-31 Multiple Vulnerabilities in BIND	Safe	Vulnerable	Vulnerable
CA-2002-29 Buffer Overflow in Kerberos Administration Daemon	Safe	Vulnerable	Safe
CA-2002-26 Buffer Overflow in CDE ToolTalk	Safe	Vulnerable	Vulnerable
CA-2002-25 Integer Overflow In XDR Library	Safe	Vulnerable	Vulnerable
CA-2002-23 Multiple Vulnerabilities In OpenSSL	Safe	Vulnerable <sup>(2)</sup>	Safe

(2) For IBM, this vulnerability affects code that comes with the AIX Toolbox for Linux.

(3) For Sun, this vulnerability affects code that comes with the Solaris Companion CD.

## Appendix: Summary of CERT/CC Advisories (Cont.)

CERT Advisory	HP OpenVMS	IBM AIX	Sun Solaris
CA-2002-20 Multiple Vulnerabilities in CDE ToolTalk	Safe	Vulnerable	Vulnerable
CA-2002-19 Buffer Overflows in Multiple DNS Resolver Libraries	Safe	Vulnerable	Vulnerable
CA-2002-18 OpenSSH Vulnerabilities in Challenge Response Handling	Safe	Vulnerable <sup>(2)</sup>	Vulnerable
CA-2002-17 Apache Web Server Chunk Handling Vulnerability	Vulnerable	Vulnerable	Vulnerable
CA-2002-11 Heap Overflow in Cachefs Daemon (cachefs)	Safe	Safe	Vulnerable
CA-2002-10 Format String Vulnerability in rpc.rwalld	Safe	Safe	Vulnerable
CA-2002-07 Double Free Bug in zlib Compression Library	Safe	Vulnerable	Vulnerable
CA-2002-03 Multiple Vulnerabilities in Many Implementations of SNMP	Safe	Vulnerable	Vulnerable
CA-2002-01 Exploitation of Vulnerability in CDE Subprocess Control Service	Safe	Safe	Vulnerable
CA-2001-35 Recent Activity Against Secure Shell Daemons	Safe	Vulnerable <sup>(2)</sup>	Safe
CA-2001-34 Buffer Overflow in System V Derived Login	Safe	Vulnerable	Vulnerable
CA-2001-31 Buffer Overflow in CDE Subprocess Control Service	Safe	Vulnerable	Vulnerable
CA-2001-30 Multiple Vulnerabilities in lpd	Safe	Vulnerable	Vulnerable
CA-2001-27 Format String Vulnerability in CDE ToolTalk	Safe	Vulnerable	Vulnerable

## Appendix: Summary of CERT/CC Advisories (Cont.)

CERT Advisory	HP OpenVMS	IBM AIX	Sun Solaris
CA-2001-21 Buffer Overflow in telnetd	Safe	Vulnerable	Vulnerable
CA-2001-15 Buffer Overflow In Sun Solaris in.lpd Print Daemon	Safe	Safe	Vulnerable
CA-2001-11 sadmind/IIS Worm	Safe	Safe	Vulnerable
CA-2001-09 Statistical Weaknesses in TCP/IP Initial Sequence Numbers	Safe	Safe	Vulnerable
CA-2001-05 Exploitation of snmpXdmid	Safe	Safe	Vulnerable
CA-2001-02 Multiple Vulnerabilities in BIND	Safe	Vulnerable	Vulnerable
CA-2000-21 Denial-of-Service Vulnerabilities in TCP/IP Stacks	Safe	Vulnerable	Safe
CA-2000-20 Multiple Denial-of-Service Problems in ISC BIND	Safe	Vulnerable	Safe
CA-2000-06 Multiple Buffer Overflows in Kerberos Authenticated Services	Safe	Vulnerable	Safe