



SecurityTrackerSM Statistics

April 2001 – March 2002

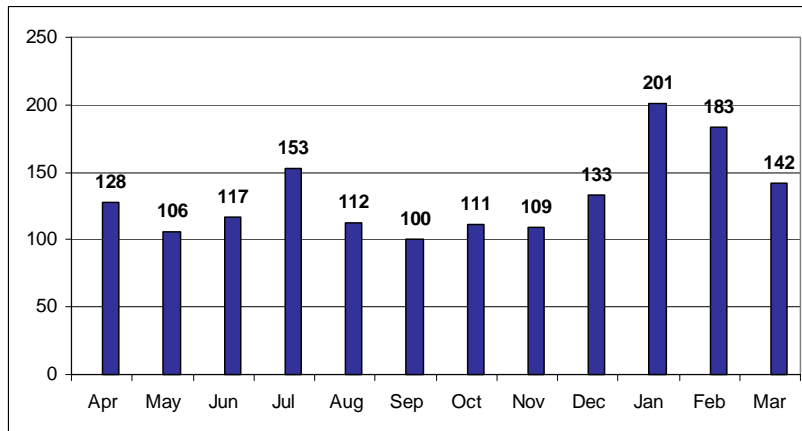
Introduction

The SecurityTracker security intelligence service is a premier vulnerability notification service created to help customers keep track of the latest vulnerabilities. The public web site (<http://www.securitytracker.com/>) provides free vulnerability information. A subscription-based service is also available to provide timely and customized notices. SecurityTracker was launched in April 2001.

In the first twelve months of operation, SecurityTracker issued 2704 alerts warning the Internet community of 1595 vulnerability reports covering 1175 products from 700 vendors. This document presents some of the statistics from our vulnerability alert service. This document can be downloaded from the SecurityTracker web site (<http://securitytracker.com/learn/statistics.html>).

The Overall Picture

We issued an average of 30 primary alerts¹ per week for a total of 1595 primary alerts during the year. January was the busiest month, followed by February. September and May were the slowest months.



Total Number of Primary Alerts Per Month

¹ A primary alert is defined as the first posting about a vulnerability on SecurityTracker. These primary alerts are typically issued based on reports from independent researchers, hackers, and security groups, but are sometimes issued by the vendors themselves. A secondary alert is a follow-up posting to an original primary alert. Secondary alerts typically include vendor fix notices, exploit information, or additional details.



The Top Ten Vendors

The following table shows the top ten vendors with the most number of vulnerability alerts.

Vendor	Total	Percentage
Microsoft	187	11.7%
Sun	42	2.6%
HP	40	2.5%
IBM	40	2.5%
Cisco	35	2.2%
Caldera/SCO	24	1.5%
Oracle	19	1.2%
Apache Software Foundation	13	0.8%
Trend Micro	13	0.8%
Netscape	10	0.6%
Network Associates	10	0.6%
Red Hat	10	0.6%

Top Ten Vendors² (Number of Total Vulnerability Alerts)

Some of the highlights of the Top Ten vendor data are listed below.

- The "Top Ten" vendors, as measured by the number of primary vulnerability Alerts for their products, were responsible for nearly 28% of all the Alerts.
- Microsoft takes the undisputed gold medal, with 187 vulnerability alerts – a whopping 11.7% of all product vulnerability alerts, and more than four times the next vendor. This gap widened during the second half of the year, in comparison with the first 6 months.
- With the exception of Cisco, all of the vendors on the Top Ten list were software manufacturers.
- Network Associates joined TrendMicro as the only security vendors to make the Top Ten list.

² There was a 3-way tie for 10th place.



Vulnerability Topics

Vulnerabilities in application software products made up the bulk of the alerts, followed by operating system software bugs and then hardware device flaws.

It is interesting to note that 86% of all vulnerability alerts were for application software, with the remaining split about evenly between operating systems and hardware devices.

The most often vulnerable category of product was web server and related applications³, such as common gateway interface (CGI) scripts and web-based applications. Interestingly, this was followed by security software. Mail server applications ranked third while web browsers ranked fourth.

The following three tables rank all of the application, operating system, and device vulnerability categories.

Topic	Total	Percentage
Application (Generic)	414	25.9%
Application (Web Server/CGI)	364	22.8%
Application (Security)	151	9.4%
Application (E-mail Server)	76	4.8%
Application (Web Browser)	64	4.0%
Application (File Transfer)	52	3.3%
Application (Database)	41	2.6%
Application (E-mail Client)	37	2.3%
Application (Commerce)	30	1.9%
Application (Multimedia)	30	1.9%
Application (Firewall)	29	1.8%
Application (File Transfer/Sharing)	23	1.4%
Application (Forum/Board/Portal)	13	0.8%
Application (Instant Messaging/IRC/Chat)	13	0.8%
Application (News)	11	0.7%
Application (Directory)	10	0.6%
Application (Game)	6	0.4%
Application (VPN)	4	0.3%
Application (Calendar)	2	0.1%
Application (VoIP)	2	0.1%
Application (Certificate Management)	1	0.1%

Application Software Vulnerabilities

³ Any application that did not fall into a more specific application category was grouped under the "Application (Generic)" category. As a result, that category is not particularly relevant when reviewing the statistics.



SecurityTrackerSM Statistics

April 2001 – March 2002

Topic	Total	Percentage
Device (Router/Bridge/Hub)	71	4.4%
Device (Firewall)	8	0.5%
Device (Printer)	4	0.3%
Device (Embedded Server/Appliance)	3	0.2%
Device (Phone)	3	0.2%
Device (Phone/FAX)	3	0.2%
Device (Embedded Server)	2	0.1%
Device (Intrusion Detection)	2	0.1%
Device (Encryption/VPN)	1	0.1%
Device (Multimedia)	1	0.1%
Device (PDA)	1	0.1%
Device (VPN)	1	0.1%

Hardware Device Vulnerabilities

Topic	Total	Percentage
OS (UNIX)	51	3.2%
OS (Microsoft)	36	2.3%
OS (Linux)	19	1.2%
OS (Mac)	8	0.5%
OS (Other)	7	0.4%

Operating System Software Vulnerabilities

Vulnerability Impacts

The most often reported vulnerability impact was one of the more serious impacts – remote execution of arbitrary code, affecting 27% of the product alerts. This is a change from the first 6 months of observed data (when remote denial of service conditions was the leading category).

About 16% of all alerts were for flaws that allowed remote users to gain user-level access on the system, and 8% of all alerts yielded remote root-level (or system-level) access for the intruder.

Almost one fourth of the alerts warned that a remote denial of service attack could be successful.



Type of Impact	Total	Percentage
Execution of arbitrary code via network	434	27.2%
Denial of service via network	330	20.7%
Disclosure of user information	307	19.2%
Disclosure of system information	293	18.4%
User access via network	255	16.0%
Execution of arbitrary code via local system	186	11.7%
Disclosure of authentication information	166	10.4%
Root access via local system	163	10.2%
Modification of system information	125	7.8%
Root access via network	125	7.8%
User access via local system	105	6.6%
Host/resource access via network	104	6.5%
Modification of user information	101	6.3%
Denial of service via local system	72	4.5%
Modification of authentication information	15	0.9%
Not Specified	1	0.1%

Type of Impact

Vulnerability Causes

While "buffer overflows" instinctively come to mind when thinking of the source of vulnerability defects, it was fundamental access control flaws that topped the list at 30% of all alerts. An access control error is one in which the product does not properly restrict the access of a user to a particular object, such as a piece of information or a control function.

The second most often occurring flaw (at over 27% of all alerts) was input validation errors. This type of flaw typically involves the lack of proper decoding of user-supplied input string. The well-publicized Nimda worm exploited an input validation flaw to traverse a web server directory and execute commands on the web server.

Ranking at third (with 20% of all alerts) was buffer overflows or boundary errors. These common errors typically allowed users to either crash the product or execute arbitrary code on the product, the latter of which frequently allowed for further exploitation.



SecurityTrackerSM Statistics

April 2001 – March 2002

Cause	Total	Percentage
Access control error	478	30.0%
Input validation error	440	27.6%
Boundary error	316	19.8%
State error	244	15.3%
Exception handling error	182	11.4%
Authentication error	108	6.8%
Configuration error	73	4.6%
Resource error	72	4.5%
Not specified	26	1.6%
Randomization error	12	0.8%

Type of Cause

Note that many alerts included more than one cause, which is why the sum of the percentages in the above table exceeds 100%. Also note that we do not categorize "poor design" or "design flaws," as design errors can occur across the board and manifest themselves as a variety of different errors.



Quality of Vendor Advisories

While not derived from the data, this section describes some subjective observations collected during the past year of vulnerability reporting.

Of the larger vendors, Microsoft was consistently the most descriptive in describing the vulnerabilities for their products. While the e-mail versions of their bulletins are now only cursory, the web versions are useful. They routinely describe the problem in reasonable detail and provide a mini-FAQ within each advisory. On the down side, Microsoft sometimes elects to fix security vulnerabilities without issuing an advisory, choosing to issue a Knowledge Base (KB) article instead. However, the KB articles still tend to be useful.

At the other end of the spectrum, HP was the least descriptive in addressing the nature of the vulnerabilities reported in their advisories, and may even be characterized as misleading in some cases. HP often used the term "denial of service" to summarize a whole range of impacts, including remote root access.

Over the past year, Novell retains the honor of having released the vaguest vulnerability report we have encountered, warning of an unspecified problem in GroupWise and failing to indicate what type of impact may be experienced if the problem is exploited. For the original alert, see: <http://www.securitytracker.com/alerts/2001/Aug/1002199.html>.

Unfortunately, many vendors still do not provide security alerts. This may be understandable for small vendors, but it is disconcerting to know that many large vendors do not readily provide security alerts via an open e-mail list or central web site, instead relegating them to technical notes that essentially get lost within a larger knowledge base. Notable amongst this group is IBM and Novell.



SecurityTrackerSM Statistics

April 2001 – March 2002

For More Information About SecurityTracker

Public Web Site

Our public web site can be viewed at: <http://www.securitytracker.com/>

Free Newsletter

You may subscribe to our free weekly e-mail vulnerability alert newsletter by signing up at: http://securitytracker.com/signup/signup_now.html.

Free Headlines

You may place SecurityTracker headlines on your web site for free by joining our Affiliate Program. Sign up at: <http://www.securitytracker.com/learn/affiliate.html>.

Customized Alert Service

You may purchase a SecurityTracker subscription service. For more information, see our web site at: <http://www.securitytracker.com/server/info?8765+learn/premium.html>.

Or, you can contact our sales department via email at: sales@securitytracker.com.

Additional Information

For any inquiries about this report, our company, or our services, you may contact us via email at: info@securitytracker.com.