

Testing for the Top Twenty Internet Security Vulnerabilities

Each of the Top Twenty vulnerable services is software that has a set of one or more specific programming errors or insecure features. These errors and features can be exploited by remote attackers, often to take control of systems that have not fixed or disabled the vulnerable software. The Top Twenty team grouped the errors and features together because, in most cases, the entire set of problems in each service can be corrected through one or a small number of steps.

Group 1 – The Scanner Vendors and MITRE

Testing for the Top Twenty, on the other hand, requires that each important programming error and insecure feature be checked individually. To identify the specific tests that were required, we assembled a team of nearly 70 people, in two groups. Group 1 came from the vendors of vulnerability scanning tools. The members included:

- Gerhard Eschelbeck of Qualys
- Renaud DeRaison of Nessus
- Bob Todd of SARA
- Harold Toomey of Symantec
- Jamie Lau and Chris Klaus of Internet Security Systems
- Dave Cole and John Bock of Foundstone, and
- Steve Christey of MITRE

As a first step, each vendor provided a list of the CVE numbers (see explanation below) corresponding with all the vulnerabilities that vendor considers as “most critical.” They were not limiting themselves to the Top Twenty.

CVE: Common Vulnerabilities and Exposures

Steve Christey of MITRE is as included not because MITRE provides a scanner, but because MITRE is the home of the critical resource that made this project possible – the Common Vulnerabilities and Exposures (CVE) project (<http://cve.mitre.org>). CVE is a community project, funded by the General Services Administration and several other Federal agencies, that gains industry agreement on common names and numbers for security vulnerabilities. Without CVE, there would have been no straightforward

way to bring together the knowledge and priority list of the vendors, because each vendor uses different descriptions for the vulnerabilities it tests. Steve Christey also provided a supplemental list of very important vulnerabilities, that were not on the vendors' lists, and helped shape the final Top Twenty CVE selection.

Working together, Group 1 arrived at a list of approximately 250 CVE numbers that they believed were critical.

Group 2: Security Practitioners from all around the globe.

Group 2, a collection of security practitioners from all over the world, prioritized the 250 CVEs.

Members of Group 2 include

| | |
|---|--|
| Charles Ajani, Standard Chartered Bank, London, UK | Kevin Liston, AT&T, Columbus OH |
| Steven Anderson, Computer Sciences Corporation, North Kingstown RI | André Mariën, Ubizen, Belgium |
| John Benninghoff, RBC Dain Rauscher, Minneapolis MN | Fran McGowran, Deloitte & Touche, Dublin, Ireland, UK |
| Layn Bro, BAE Systems, Denver CO | Derek Milroy, Zurich North America, Chicago IL |
| Thomas Buehlmann, Phoenix AZ | Bruce Moore, Canadian Forces Network Operations Center, DND, Ottawa Canada |
| Ed Chan, NASA Ames Research Center, San Jose CA | Castor Morales, Ft. Lauderdale FL |
| Andrew Clarke, Computer Solutions, White Plains NY | Luis Perez, Boston MA |
| Brian Coogan, ManageSoft, Melbourne Australia | Reg Quinton, University of Waterloo, Ontario Canada |
| Paul Docherty, Portcullis Computer Security Limited, UK | Bartek Raszczyk, UWM Olsztyn, Olsztyn Poland |
| Arian Evans, U.S. Central Credit Union, Overland Park KS | Teppo Rissanen, Plasec Oy, Helsinki Finland |
| Rich Fuchs, Research Libraries Group, Mountain View CA | Alan Rouse, N2 Broadband, Duluth GA |
| Mark Gibbons, International Network Services, Minneapolis MN | Denis Sanche, PWGSC ITSD/IPC, Hull, QC Canada |
| Dan Goldberg, Rochester NY | Felix Schallock, Ernst & Young, Vienna, Austria |
| Shan Hemphill, Sacramento CA | Gaston Sloover, Fidelitas, Buenos Aires Argentina |
| Michael Hensing, Charlotte, NC, Microsoft | Arthur Spencer, UMASS Medical School, Worcester MA |
| Simon Horn, Brisbane Australia | Rick Squires |
| Bruce Howard, Kanwal Computing Solutions, Jiliby NSW Australia | Jeff Stehlin, HP |
| Tyler Hudak, Akron OH | Koon Yaw TAN, Infocomm Development Authority of Singapore, Singapore |
| Delbert Hundley, MPRI Division of L-3COM, Norfolk VA | Steven Weil, Seitel Leeds & Associates, Seattle WA |
| Chyuan-Horng Jang, Oak Brook IL | Lance Wilson, Time Warner Cable/Broadband IS, Orlando FL |
| Kim Kelly, The George Washington University, Washington DC | Andrew Wortman, Naval Research Laboratory, Washington DC |
| Martin Khoo, Singapore Computer Emergency Response Team (SingCERT), Singapore | Carlos Zottman, Superior Tribunal de Justiça, Brasilia Brazil |
| Susan Koski, Pittsburgh PA | |

In the final step, leaders of the team building the Top Twenty sorted the high-priority vulnerabilities into those that relate to the Top Twenty and others. The scanners use this list to check systems for Top Twenty Vulnerable Services.

***Second Tier Critical
Vulnerabilities List
Coming in 2003***

The remaining high-priority vulnerabilities will form the core of a new Second Tier Critical Vulnerabilities that the Top Twenty team plans to compile and publish early in 2003.