



Contact:
Alan Paller: paller@sans.org, (301) 951-0102 ext. 108

GLOBAL SECURITY EXPERTS JOIN TO ISSUE ANNUAL UPDATE OF SANS TOP 20 MOST CRITICAL INTERNET VULNERABILITIES REPORT

New Report Finds Significant Shifts in Software Being Targeted By Attackers

LONDON, UK. – The SANS Top 20, produced since 2000, is the security experts' consensus of the most critical security vulnerabilities. These vulnerabilities are the programming flaws, contained in popular software packages, that deserve immediate attention from security professionals, CIOs and auditors to protect Internet-connected systems from widespread attacks.

New Attack Patterns Reflected in the 2005 Top 20

The 2005 Top 20 reflects a significant shift from prior years in cyber attack targets. For five years, the majority of attacks targeted operating systems like UNIX and Windows and Internet services like web servers and mail systems. In 2005, however, a new wave of attacks concentrated on application programs. The most noticeable set of applications that are being targeted by attackers are the backup and recovery tools and the antivirus and other security tools that most organizations think are keeping them safe from attacks and from loss of data. Now many of those systems have been shown to have critical vulnerabilities.

"We are seeing a trend to exploit not only Windows, but other vendor programs installed on large numbers of systems," says Rohit Dhamankar, lead security architect at 3Com's TippingPoint division. *"These include backup software, anti-virus software, database software and even media players. Flaws in these programs put critical national and corporate resources at risk and have the potential to compromise the entire network."*

"In Qualys's weekly vulnerability scans, covering millions of computer systems in more than 20 countries, we are finding significant numbers of vulnerabilities in popular applications," noted Gerhard Eschelbeck, Chief Technology Officer of Qualys.

Jerry Dixon, Director of the US-CERT, confirmed those vulnerabilities are being actively targeted by criminals, *"The US-Cert received reports of important system compromises using vulnerabilities in backup products within a few days of the public disclosure of vulnerabilities in those products."*

A second important shift in the Top 20 is public recognition of the critical vulnerabilities that are found in network devices such as routers and switches that form the backbone of the Internet. Network devices often have on-board operating systems and can be programmed just like computers. Compromises of network devices can provide attackers one of the most fruitful platforms for eavesdropping and launching targeted attacks.

The Skyrocketing Threat of Targeted Attacks

On June 16, 2005 the National Infrastructure Security Co-Ordination Centre in the United Kingdom issued a public advisory describing a series of targeted attacks against the UK central government and commercial organizations “for the purpose of gathering and transmitting otherwise privileged information.” The UK advisory pointed to email born attacks, but equally devastating attacks are being carried out against US government and military-contractor sites using vulnerabilities like those reported in SANS Top 20.

"In prior years, the attackers may have been young people out to make a name for themselves. Today the attacks are being carried out by organized professionals with financial goals. This is creating a malicious market place through which the capability to damage us will become more readily available." said NISCC Director Roger Cumming.

The 2005 SANS Top 20

The 2005 SANS Top 20
The Most Critical Internet Security Vulnerabilities
See www.sans.org/top20/ for details

Top Vulnerabilities in Windows Systems

- W1. Windows Services
- W2. Internet Explorer
- W3. Windows Libraries
- W4. Windows Office and Outlook Express
- W5. File Sharing Applications
- W6. Windows Configuration Weaknesses

Top Vulnerabilities in Cross-Platform Applications

- C1. Backup Software
- C2. Anti-virus Software
- C3. PHP-based Applications
- C4. Database Software
- C5. DNS Software
- C6. Media Players
- C7. Instant Messaging Applications
- C8. Web Browsers
- C9. Other Cross-platform Applications

Top Vulnerabilities in UNIX Systems

- U1. UNIX Configuration Weaknesses
- U2. Mac OS X

Top Vulnerabilities in Networking Products

- N1. Cisco IOS-based Products
- N2. Cisco non-IOS Products
- N3. Cisco Devices Configuration Weaknesses

What Makes A Vulnerability Critical?

According to Rohit Dhamankar, lead security architect at TippingPoint, a division of 3Com, and project manager for the SANS Top 20,

“Vulnerabilities on this list meet four requirements: (1) they affect a large number of users, (2) they have not been patched on a substantial number of systems, (3) they allow computers to be controlled by a remote, unauthorized user, (4) sufficient details about the vulnerabilities have been posted to the Internet to enable attackers to exploit them.”

In other words, they are the “low hanging fruit” for nation states, terrorists, and organized crime organizations who want to steal sensitive information.

“These critical vulnerabilities are widespread and many of them are being exploited, right now, in our homes and in our offices” according to Alan Paller, Director of Research for SANS Institute. *“We’re publishing this list as a red flag for individuals as well as IT departments. Too many people are unaware of these vulnerabilities, or mistakenly believe their computers are protected.”*

“With all the attention that is given to high-profile threats or targeted attacks, it is easy to lose sight of the fact that even highly-sophisticated attackers frequently attempt to exploit well-known vulnerabilities,” says Julie Spallin, Director of the Canadian Cyber Incident Response Centre. *“As part of the Government of Canada’s efforts to enhance cyber security, we are working with our critical infrastructure community to reduce their overall cyber risk. In this effort, the SANS Top 20 continues to be an excellent reference that can help focus limited resources on the most commonly-attacked vulnerabilities.”*

Weekly updates of the Top 20

SANS summarizes all critical new vulnerabilities each week and distributes the list and details, at no cost, to 120,000 security professionals around the world. The weekly e-letter, called @RISK, also includes detailed guidance on how to patch or work around each critical vulnerability, a list of *all* new vulnerabilities discovered during that week, and new exploits that are in the wild. If you would like to be included in the distribution list, visit <http://www.sans.org/newsletters/> and choose @RISK.

The Top 20 Team

The team that collaborated to compile and verify the 2005 Top 20 includes representatives from seven key security organizations:

- Representing the government community are the **U.S. Computer Emergency Response Team (US-CERT)** at the Department of Homeland Security, the **British Government’s National Infrastructure Security Co-Ordination Centre (NISCC)**, and **Canada’s Cyber Incident Response Centre**. Representatives from US intelligence agencies also provided essential information on which vulnerabilities are being actively targeted.
- Representing the intrusion prevention expert community, and leading the SANS team to the Top 20 effort, is **Rohit Dhamankar of TippingPoint**. TippingPoint tracks all critical vulnerabilities as an essential step in continuously updating its intrusion prevention products with protection against new threats. The analysis done by TippingPoint provides deep understanding of how critical vulnerabilities work and how they can be exploited.
- Representing the vulnerability management expert community is **Gerhard Eschelbeck of Qualys**. Qualys tracks all new vulnerabilities as an essential element of its process of checking

more than 2,000,000 computers each week to see whether any vulnerabilities are present. Qualys provided valuable information that helped determine that these vulnerabilities were still widespread.

- Representing the **SANS Internet Storm Center** community are **Marcus Sachs and Johannes Ullrich**. SANS Internet Storm Center monitors the Internet using more than 6,000 sensors managed by volunteers around the world, providing early warning of worms and other widespread cyber attacks. It also monitors attacks through voluntary reporting and nightly analysis to help illuminate new types of attacks appearing on the Internet.
- More than twenty other security experts from countries around the world helped evaluate the vulnerabilities and ensure the documentation was correct. They are listed at the end of the Top 20 report.

##

SANS Institute was established in 1989 and has become the largest source for information security training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system -- Internet Storm Center. SANS Institute began as a cooperative research and education organization and now reaches more than 165,000 security professionals, auditors, system administrators, network administrators, chief information security officers, and CIOs. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community. Further information about SANS is available at <http://www.sans.org>.