ComputerWeekly

N° and issue date : 41005 - 05/10/2004
Circulation : 133000
Periodicity : Weekly
Page : 1
ComputerWeekly_41005_4_304.pdf
Size : 78 %
Web Site: http://www.computerweekly.com

Force suppliers to act on vulnerabilities or pay the price, leading security experts warn users

Users face five years of patching pain as security flaws keep rising

Bill Goodwin
bill.goodwin@rbi.co.uk

Businesses will face another five years of battling with serious security vulnerabilities and complex patching regimes, the Sans Institute will warn this week.

Known vulnerabilities in commercial software have doubled during the past year to more than 2,000, research by members of the Sans Institute reveals.

The US-based institute is a co-operative research and education body. Its vulnerability research has been compiled by 200 of the world's leading security experts from suppliers, government, universities and corporate users.

Although Windows 2003 is supplied with security locked down, it will be at least 2009 before most software suppliers start to deliver packages taking advantage of this, perpetuating patching difficulties, Sans predicts.

The institute is urging organisations to step up pressure on suppliers to deliver secure code as it prepares to publish its analysis of the top 20 security vulnerabilities facing IT departments on Friday (8 October).

"Suppliers are continuing to sell systems full of critical vulnerabilities and if we as users don't act together to make them do a better job, we will be living with the same problems, only worse, for 20 years," said Alan Paller, director of research at Sans.

He urged users to add clauses requiring suppliers to scan systems for vulnerabilities and to lock down security features to their contracts.

The practice is being pioneered by the US government, which has placed orders for tens of thousands of pre-scanned preconfigured desktop PCs.

"The key to any security is configuration. You have two ways of doing it. You can tell all your users to do it, or you can tell the suppliers to do it," said Paller. "The suppliers are kicking and screaming and doing it reluctantly. But they prefer to do it than to lose the revenue."

John Meakin, group head of information security at Standard Chartered Bank, said there were too many packaged software products on sale, which fail to follow basic security practices.

"The corporate world really ought to be saying 'no longer will we accept deficient security functionality', quite apart from the issue of vulnerabilities," he said.

The top 20 list, to be unveiled at a high profile conference at the DTI, will provide firms with a benchmark to secure their organisations, prioritise patching, and

→ continued on p4

The top vulnerabilities in 2004

Windows vulnerabilities

- **Internet messaging – remotely exploitable vulnerabilities and the potential of abuse by staff**
- **Windows remote access services – many are notoriously insecure, such as Netbios network shares, and remote procedure calls**
- **File-sharing applications – peer-to-peer software can provide a back door into company systems**

Unix/Linux vulnerabilities

- **Bind domain name system – at risk from denial-of-service attacks and buffer overflows**
- **Version control systems – can be exploited by hackers to leave back doors in systems**
- **Simple Network Management Protocol – can be used by hackers to launch denial-of-service attacks.**

Source: Sans Institute

ComputerWeekly

N° and issue date : 41005 - 05/10/2004
Circulation : 133000
Periodicity : Weekly
ComputerWeekly_41005_4_304.pdf
Web Site: http://www.computerweekly.com
Page : 4
Size : 98 %

SECURITY

Vulnerabilities of the past still haunt present

← continued from p1

will offer detailed technical advice on correcting vulnerabilities.

New critical problems facing IT directors this year include instant messaging software and peer-to-peer networks, which can provide a back door for hackers and malicious code, and the Microsoft LSASS vulnerability exploited by the Sasser worm, which is still widespread.

The past 12 months have seen the emergence of a new generation of vulnerabilities, which affect multiple applications and cannot be fixed by a single patch.

"We are still dealing with the sins of the past. The reality is that, when you look at the industry, there is tremendous movement going into making the security the measure of software," said Gerhard Eschelbeck, chief technology officer at Qualys, and one of the Sans advisers.

Sans says the number of vulnerabilities will peak next year.

→ www.sans.orgtop20
→ The writing on the wall, p26

Users fail to take action on known flaws

IT departments are failing to secure their systems against security vulnerabilities that have been common knowledge for years, a study by the Sans Institute reveals.

The Sans top 20 list of the most critical security vulnerabilities, to be unveiled this week, highlights problems that were first identified by the institute five years ago.

They include:

- Simple Network Management Protocol can be exploited by hackers to misdirect router traffic or bring down a network
- DCom RPC vulnerability exploited by the Sasser worm
- Apache junk encoding memory corruption vulnerability, which allows buffer overflow attacks

The latter two were identified last year, and are still ubiquitous.