

## Join the Dark Side

Click [here](#) for the DR Weekly Newsletter, and [here](#) to enjoy site member benefits



DATE: April 14, 2008

LIVE EVENT: **Ethernet Expo Europe**

LOCATION: The Business Design Centre, Islington, ...

[More Information](#)

[Home](#) > [Dark Reading News Feed](#) > [Application and Perimeter Security](#)

SEARCH [▶ ADVANCED SEARCH](#)

# Codemicon Upgrades Platform

## Codemicon announces next-generation security testing software with unmatched ability to identify flaws before products ship

APRIL 1, 2008 | SAN JOSE, Calif. and OULU, Finland -- Codemicon, Ltd. today announced DEFENSICS 3.0, the third generation of its innovative security and quality testing platform that allows networked product and service manufacturers and vendors to quickly identify and fix flaws by catching the problems before their offerings ever reach the market.

"It is clear that traditional testing processes continue to fail vendors and their customers. News reports of security breaches and attacks that cripple businesses and their reputations keep emerging and, frankly, many end users have just had it," said Ari Takanen, Codemicon co-founder and chief technology officer. "Our latest DEFENSICS test platform offers an even faster, more effective way to expose and fix security-critical product and service flaws before they harm customers' businesses or compromise consumer information. By using our tools, vendors can deliver better quality, reduce their time to market and minimize or eliminate the need to patch or recall their products, a key advantage as customers reward vendors that deliver superior products."

[Codemicon Ltd.](#)

- [DISCUSS](#)
- [EMAIL](#)
- [PRINT](#)
- [LINK/REPRINT](#)
- [SHARE](#)
- [RSS](#)

### RELATED

#### VIDEO



**Dan Kaminsky,**  
Director -  
Penetration Testing,  
IOActive

[PLAY](#) (06:49)

Flaws: Back to the Future



**Jennifer Granick,**  
Director - Cyberlaw  
Clinic, Stanford Law  
School

[PLAY](#) (05:33)

### KEYHOLE

Security Issues Limit Telecommuting  
Hacked in Two Minutes

Attention, Stolen Credit Card Shoppers

[MORE KEYHOLE](#)



[DISCUSS](#) [EMAIL](#) [PRINT](#) [LINK/REPRINT](#) [SHARE](#)

## MESSAGE BOARDS

[Discuss this story >](#)

### Is That Legal?

#### NEWS ANALYSIS

- [Black Hat Researcher Hacks Biometric System](#) 3/31/2008

- [Tech Insight: Keeping Your Thumb on Thumb Drives](#) 3/28/2008

#### RESEARCH

- [Web App Firewalls: Who's Doing What](#)

- [Web Services & Grid Computing: Synergy Rules](#)

- [MicroTCA & AdvancedMC: Delivering on the Promise](#)

- [Service Delivery and XML: The Path to Carrier SOA](#)

- [Mobile Malware: The Enterprise at Risk](#)

#### WEBINAR ARCHIVE

- [From IM to Social Networking: Securing Employee Use of the Web](#) 3/26/2008

- [Security Update: eCards, Email Threats and Compliance](#) 10/24/2007

#### COLUMNS

- [Hacking WiFi](#) 3/13/2008

- [When Bad Tech Leads to Worse Results](#) 3/12/2008

#### REPORTS

- [Ten Myths About Identity Fraud](#) 2/12/2008

- [The World's Biggest Botnets](#) 11/9/2007

## BUGS

### ENTERPRISE VULNERABILITIES

**Vulnerability:** IBM AIX  
**Published:** 2008-04-01  
**Severity:** HIGH  
**Description:** stack-based buffer overflow in the reboot program on ibm aix 5.2 and 5.3 allows local users in the shutdown group to gain privileges.

**Vulnerability:** IBM AIX  
**Published:** 2008-04-01  
**Severity:** HIGH  
**Description:** the lsmcode program on ibm aix 5.2, 5.3, and 6.1 does not properly handle environment variables, which allows local users to gain privileges, a different vulnerability than cve-2004-1329.

**Vulnerability:** IBM AIX  
**Published:** 2008-04-01  
**Severity:** HIGH  
**Description:** the nddstat programs on ibm aix 5.2, 5.3, and 6.1 do not properly handle environment variables, which allows local users to gain privileges by invoking (1) atmstat, (2) entstat, (3) fddistat, (4) hdlcstat, or (5) tokstat.

**Vulnerability:** IBM AIX  
**Published:** 2008-04-01  
**Severity:** MEDIUM  
**Description:** the kernel in ibm aix 6.1 allows local users with probevue privileges to read arbitrary kernel memory and obtain sensitive information via unspecified vectors.

**Vulnerability:** IBM AIX  
**Published:** 2008-04-01  
**Severity:** MEDIUM  
**Description:** the wpar system call implementation in the kernel in ibm aix 6.1 allows local users to cause a denial of service via unknown calls that trigger "undefined behavior."



STOP THE BAD.  
ACCELERATE  
THE GOOD.

BLUE COAT  
YOUR BUSINESS.

See why 93 of  
the top 100 from the  
FORTUNE Global 500®  
depend on Blue Coat  
for WAN application  
delivery >>

Blue Coat

ADVERTISING LINKS

## DARK READING MARKETPLACE

**SOLVE MORE ISSUES on the first call. Try WebEx FREE**

ZAP REMOTE SUPPORT ISSUES! Crush Support Log Jams! BLAST THROUGH FIREWALLS! Try WebEx REMOTE SUPPORT

**Succeeding with Seagate® is an Easy Decision.**

Register for the Seagate® Partner Program and Win a Barracuda® 1-TB drive!

**Anti Spam/Virus for Exchange Server 2000/2003/2007**

SPAMfighter for Exchange Servers is the easy-to-use spam and virus filter. Try it free for 30 days

**FREE Application Discovery Tool from Sophos**

Scan your network for VoIP, IM, games and other potentially unwanted applications.

**FREE Sophos Threat Detection Test**

Scan for viruses, spyware & adware. Is your AV catching everything?

[BUY A LINK NOW](#)



**BRIEFING CENTERS**

POWERFUL INFORMATION AT YOUR FINGERTIPS (SPONSORED LINKS)



- Understand the changing role of the CIO
- 
- 
- 

**TAG CLOUD**

Application Security | Attacks / Exploits / Threats | Authentication | Black Hat | Botnets | Browser security | Computer crime | Consultants | Content filtering | Cross-site scripting | DOS | Encryption | Firewalls | Host Protection | Identity management | IDS | Industry Trends | IPS | Law enforcement | Legal & Regulatory Topics |

Copyright © 2008 United Business Media LLC - All rights reserved.

[Privacy Policy](#) | [Terms of Use](#) | [Help](#) | [Back to Top](#)

[Legislation](#) | [Malware](#) |

[Market Research](#) | [McAfee](#) |

[Messaging Security](#) |

[Microsoft](#) | [Penetration testing](#)

| [Penetration testing](#) |

[Perimeter](#)

[Security](#) | [Phishing](#) |

[Policy management](#) | [Rootkits](#)

| [Security](#)

[Administration /](#)

[Management](#) |

[Security Industry](#)

| [Security Services](#) | [Social](#)

[engineering](#) | [Spam](#) | [Storage](#)

[Security](#) | [Stored data losses](#) |

[Trojans](#) | [User privacy](#) |

[Viruses](#) |

[Vulnerabilities](#) |

[Vulnerability](#)

[assessment](#) |

[Vulnerability](#)

[management](#) |

[Vulnerability Management](#) |

[Web application firewall](#) | [Web](#)

[services security](#) | [Wireless](#)

[security](#) | [Worms](#)

## FREE NEWSLETTERS

[Dark Reader Weekly  
Newsletter](#)

[Dark Reading Daily  
Newsletter](#)

[MORE INFO](#)

[RSS FEED](#) | [ARCHIVE](#) | [FREE NEWSLETTER](#) | [ORDER REPRINTS](#) | [ADVERTISE WITH US](#) | [TECHWEB](#) | [CONTACT US](#) | [USER PREFERENCES](#) | [HELP](#)

[HOME](#) | [NEWS](#) | [OPINION](#) | [VIDEO](#) | [TALK](#) | [EVENTS](#) | [JOB SEARCH](#) | [PAID RESEARCH](#) | [WHITE PAGES](#) | [REGISTER](#) | [SPONSOR](#) | [ABOUT US](#)

### Companies

[3Com](#) (15), [Aventail](#) (7), [CA](#) (14), [Check Point](#) (28), [Cisco](#) (134), [Enterasys](#) (5), [F-Secure](#) (6), [F5](#) (5), [HP](#) (13), [IBM](#) (111), [Intel](#) (6), [ISS](#) (30), [Juniper](#) (36), [Alcatel-Lucent](#) (1), [McAfee](#) (153), [Microsoft](#) (1096), [NetIQ](#) (2), [Nokia](#) (3), [Nortel](#) (6), [Oracle](#) (41), [Qualys](#) (2), [RSA](#) (38), [Secure Computing](#) (17), [Sun](#) (7), [Symantec](#) (265), [Trend Micro](#) (23), [VeriSign](#) (31)

### Application and Perimeter Security

[802.11x](#) (44), [Anomaly detection](#) (74), [Anti-spam](#) (129), [Application quality assurance](#) (27), [Application scanning](#) (126), [Auditing](#) (27), [AVDL](#) (1), [Buffer overflows](#) (98), [CERT](#) (7), [Consultants](#) (190), [Cross-site scripting](#) (152), [CVE](#) (7), [Database encryption](#) (53), [Digital vaults](#) (8), [DOS](#) (176), [EAP/LEAP](#) (1), [Email gateways](#) (158), [Encryption](#) (114), [Filtering](#) (48), [Firewalls](#) (275), [FIRST](#) (1), [HIPAA](#) (96), [Host-based IDS](#) (43), [Host/server configuration](#) (14), [Host/server encryption](#) (8), [IDS](#) (13), [IDS](#) (155), [IM](#) (66), [IPS](#) (248), [ISO 17799](#) (8), [Key management](#) (59), [Least-privilege user](#) (43), [License management](#) (30), [Malware](#) (1160), [NAC](#) (260), [Network IDS](#) (32), [NIST](#) (16), [OWASP](#) (10), [OWASP](#) (14), [Patch management](#) (277), [PCI](#) (168), [Penetration testing](#) (181), [Phishing](#) (580), [PKI](#) (41), [Rootkits](#) (98), [SAML](#) (2), [Software metering](#) (3), [Source-code auditing](#) (71), [SOX](#) (82), [SSL](#) (165), [Systems integrators](#) (7), [VPNs](#) (238), [Vulnerability assessment](#) (653), [Web App Security Consortium](#) (17), [Web App Security Consortium](#) (8), [Web application firewall](#) (77), [Web services security](#) (472), [WLANs](#) (326), [Worms](#) (263), [WPA](#) (14), [XML](#) (27)

### Desktop Security

[Anti-spam](#) (129), [Antivirus](#) (320), [Application Security](#) (977), [Attacks / Exploits / Threats](#) (2125), [Authentication](#) (748), [Browser security](#) (646), [Digital certificates](#) (56), [Digital signatures](#) (42), [Disk encryption](#) (53), [DRM](#) (51), [Encryption](#) (530), [File/folder encryption](#) (35), [Identity management](#) (302), [IM](#) (66), [Malware](#) (1160), [Messaging Security](#) (463), [PGP](#) (5), [Phishing](#) (580), [Rootkits](#) (98), [S/MIME](#) (2), [Security Administration / Management](#) (1496), [Social engineering](#) (306), [Spam](#) (603), [Spyware](#) (241), [Tokens](#) (65), [Trojans](#) (310), [User privacy](#) (1291), [Viruses](#) (335), [VOIP security](#) (107), [Vulnerabilities](#) (2514), [Vulnerability Management](#) (390), [Worms](#) (263)

### Discovery and management

[Anomaly detection](#) (74), [Application scanning](#) (126), [AVDL](#) (1), [Black Hat](#) (106), [COBIT](#) (8), [Consultants](#) (190), [Content filtering](#) (153), [CVE](#) (7), [End-user monitoring](#) (226), [Filtering](#) (48), [FISMA](#) (19), [HIPAA](#) (96), [Host intrusion prevention](#) (102), [Host-based IDS](#) (43), [IDS](#) (13), [IDS](#) (155), [IPS](#) (248), [ISACA](#) (1), [ISO 17799](#) (8), [Log aggregation](#) (48), [Network IDS](#) (32), [OWASP](#) (14), [OWASP](#) (10), [PCI](#) (168), [Penetration testing](#) (165), [Penetration testing](#) (181), [SAML](#) (2), [SIM/SEM](#) (169), [Source-code auditing](#) (71), [SOX](#) (82), [Vulnerability assessment](#) (653), [Vulnerability management](#) (724), [Web App Security Consortium](#) (8)

### Host security

[802.11x](#) (44), [Application quality assurance](#) (27), [Authentication](#) (748), [Backup security](#) (61), [Biometrics](#) (144), [Buffer overflows](#) (98), [Digital certificates](#) (56), [Disk encryption](#) (53), [Encryption](#) (530), [End-user monitoring](#) (226), [HIPAA](#) (96), [Host anti-spam](#) (73), [Host anti-spyware](#) (96), [Host antivirus](#) (105), [Host intrusion prevention](#) (102), [Host Protection](#) (434), [Host-based IDS](#) (43), [Host/server configuration](#) (14), [Host/server encryption](#) (8), [Host/server patching](#) (9), [IDS](#) (13), [IEEE](#) (4), [ISO 17799](#) (8), [Least-privilege user](#) (43), [License management](#) (30), [NAC](#) (260), [P2P management](#) (26), [Patch management](#) (277), [PGP](#) (14), [Port control](#) (10), [Single sign-on](#) (63), [Smart cards](#) (74), [Software metering](#) (3), [SOX](#) (82), [Systems integrators](#) (7), [TCG](#) (18), [Tokens](#) (65), [User privacy](#) (1291), [Vulnerability Management](#) (390), [WPA](#) (14)

### Security services

[Agency application](#) (2), [Application quality assurance](#) (27), [Application scanning](#) (126), [AVDL](#) (1), [COBIT](#) (8), [Consultants](#) (190), [FISMA](#) (19), [HIPAA](#) (96), [ISO 17799](#) (8), [Managed services](#) (273), [PCI](#) (168), [Penetration testing](#) (165), [PKI](#) (41), [Policy management](#) (415), [SIM/SEM](#) (169), [Source-code auditing](#) (71), [SOX](#) (82), [Systems integrators](#) (7)

### Storage Security

[AES](#) (10), [Backup security](#) (61), [COBIT](#) (8), [Database encryption](#) (53), [DES](#) (3), [Digital vaults](#) (8), [Disk encryption](#) (53), [Encryption](#) (114), [File/folder encryption](#) (35), [FIPS-140-2](#) (1), [FISMA](#) (19), [Hashing algorithms](#) (13), [HIPAA](#) (96), [Host/server encryption](#) (8), [Identity management](#) (97), [ISO 17799](#) (8), [Key management](#) (59), [Law enforcement](#) (860), [Legislation](#) (267), [Offsite backup](#) (25), [PCI](#) (168), [PKI](#) (41), [SOX](#) (82), [Stored data losses](#) (290), [Systems integrators](#) (7), [Triple DES](#) (3), [User privacy](#) (1291)

### Wireless Security

[802.11x](#) (44), [AES](#) (10), [Auditing](#) (27), [COBIT](#) (8), [Credential service provider](#) (7), [DES](#) (3), [Digital certificates](#) (56), [Digital signatures](#) (42), [DOS](#) (176), [EAP/LEAP](#) (1), [FISMA](#) (19), [Hashing algorithms](#) (13), [HIPAA](#) (96), [Host/server encryption](#) (8), [IEEE](#) (4), [IETF](#) (10), [ISO 17799](#) (8), [Key management](#) (59), [NAC](#) (260), [Network IDS](#) (32), [PCI](#) (168), [Penetration testing](#) (165), [PKI](#) (41), [Port control](#) (10), [Tokens](#) (65), [Triple DES](#) (3), [VPNs](#) (238), [Vulnerability assessment](#) (653), [WLANs](#) (326), [WPA](#) (14)