



Search US-CERT

GO

Advanced Options...

## National Cyber Alert System

### Cyber Security Bulletin SB07-211

Archive

## Vulnerability Summary for the Week of July 23, 2007

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Adaptive Business Design	SQL injection vulnerability in Infinite Responder before 1.48	unknown	<a href="#">7.5</a>	<a href="#">CVE-2007-3943</a>

-- Infinite Responder	allows remote attackers to execute arbitrary SQL commands via unspecified vectors. NOTE: some of these details are obtained from third party information.	2007-07-20		<a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">XF</a>
Apple -- Safari	Unspecified vulnerability in Safari (MobileSafari) on the Apple iPhone allows remote attackers to execute arbitrary code via unspecified vectors. NOTE: This information is based upon a vague pre-advisory. Details will be updated after the grace period has ended.	unknown 2007-07-23	<a href="#">9.3</a>	<a href="#">CVE-2007-3944</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a>
Article Directory -- Article Directory	PHP remote file inclusion vulnerability in index.php in Article Directory (Article Site Directory) allows remote attackers to execute arbitrary PHP code via a URL in the page parameter.	unknown 2007-07-25	<a href="#">9.3</a>	<a href="#">CVE-2007-4007</a> <a href="#">MILWORM</a> <a href="#">OTHER-REF</a> <a href="#">BID</a>
ASP Indir -- Dora Emlak	Multiple cross-site scripting (XSS) vulnerabilities in default.asp in Dora Emlak 1.0, when the goster parameter is set to iletisim, allow remote attackers to inject arbitrary web script or HTML via the (1) Adiniz and (2) Soyadiniz parameters; and possibly other unspecified vectors. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2007-07-25	<a href="#">7.5</a>	<a href="#">CVE-2007-3989</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a>
ASP Indir -- Dora Emlak	SQL injection vulnerability in default.asp in Dora Emlak 1.0, when the goster parameter is set to emlakdetay, allows remote attackers to execute arbitrary SQL commands via the id parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2007-07-25	<a href="#">7.5</a>	<a href="#">CVE-2007-3990</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a>
Borland Software -- Interbase	Stack-based buffer overflow in the database service (ibserver.exe) in Borland InterBase 2007 before SP2 allows remote attackers to execute arbitrary code via a long size value in a create request to port 3050/tcp.	unknown 2007-07-26	<a href="#">7.5</a>	<a href="#">CVE-2007-3566</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a>

				<a href="#">SECUNIA</a>
bwired -- bwired	SQL injection vulnerability in index.php in bwired allows remote attackers to execute arbitrary SQL commands via the newsID parameter.	unknown 2007-07-25	<a href="#">7.5</a>	<a href="#">CVE-2007-3976</a> <a href="#">MILWORM</a>
CA -- eTrust Intrusion Detection	The CallCode ActiveX control in caller.dll 3.0 before 20070713, and 3.0 SP1 before 3.0.5.81, in CA (formerly Computer Associates) eTrust Intrusion Detection allows remote attackers to load arbitrary DLLs on a client system, and execute code from these DLLs, via unspecified "scriptable functions."	unknown 2007-07-25	<a href="#">9.3</a>	<a href="#">CVE-2007-3302</a> <a href="#">IDEFENSE</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a> <a href="#">XF</a>
Centennial -- Discovery Symantec -- Discovery Numara -- Asset Manager	Centennial Discovery 2006 Feature Pack 1, which is used by (1) Numara Asset Manager 8.0 and (2) Symantec Discovery 6.5, uses insecure permissions on certain directories, which allows local users to gain privileges.	unknown 2007-07-23	<a href="#">7.2</a>	<a href="#">CVE-2007-2950</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">FRSIRT</a> <a href="#">FRSIRT</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a> <a href="#">SECUNIA</a> <a href="#">SECUNIA</a>
Cisco -- Wireless LAN Controller	Cisco 4100 and 4400, Airespace 4000, and Catalyst 6500 and 3750 Wireless LAN Controller (WLC) software before 3.2 20070727, 4.0 before 20070727, and 4.1 before 4.1.180.0 allows remote attackers to cause a denial of service (traffic amplification or ARP storm) via a crafted unicast ARP request that (1) has a destination MAC address unknown to the Layer-2 infrastructure, aka CSCsj69233; or (2) occurs during Layer-3 roaming across IP subnets, aka CSCsj70841.	unknown 2007-07-25	<a href="#">7.1</a>	<a href="#">CVE-2007-4011</a> <a href="#">CISCO</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a>
Cisco -- Wireless LAN Controller	Cisco 4100 and 4400, Airespace 4000, and Catalyst 6500 and 3750 Wireless LAN Controller (WLC) software 4.1 before 4.1.180.0 allows remote attackers to cause a denial	unknown 2007-07-25	<a href="#">7.1</a>	<a href="#">CVE-2007-4012</a> <a href="#">CISCO</a> <a href="#">BID</a>

	of service (ARP storm) via a broadcast ARP packet that "targets the IP address of a known client context", aka CSCsj50374.			<a href="#">FRSIRT</a> <a href="#">SECUNIA</a>
Citrix -- Endpoint Analysis Client Citrix -- Access Gateway Mozilla -- Firefox plugin	Multiple unspecified vulnerabilities in (1) Net6Helper.DLL (aka Net6Launcher Class) 4.5.2 and earlier, (2) npCtxCAO.dll (aka Citrix Endpoint Analysis Client) in a Firefox plugin directory, and (3) a second npCtxCAO.dll (aka CCAOControl Object) before 4.5.0.0 in Citrix Access Gateway Standard Edition before 4.5.5 and Advanced Edition before 4.5 HF1 have unknown impact and attack vectors, possibly related to buffer overflows. NOTE: vector 3 might overlap CVE-2007-3679.	unknown 2007-07-25	<a href="#">9.3</a>	<a href="#">CVE-2007-4013</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a>
Citrix -- Access Gateway	Citrix Access Gateway Advanced Edition before 4.5 HF1 allows attackers to obtain sensitive information and hijack a session via unspecified vectors related to "residual information" on a client device.	unknown 2007-07-25	<a href="#">9.3</a>	<a href="#">CVE-2007-4015</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a>
Citrix -- Access Gateway	Cross-site request forgery (CSRF) vulnerability in the web-based administration console in Citrix Access Gateway before firmware 4.5.5 allows remote attackers to perform certain configuration changes as administrators.	unknown 2007-07-25	<a href="#">7.6</a>	<a href="#">CVE-2007-4017</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a>
Computer Associates -- Unicenter Enterprise Job Manager Computer Associates -- Unicenter Application Performance Monitor Computer Associates -- Unicenter NSM Wireless Network Management	Stack-based buffer overflow in the Message Queuing Server (Cam.exe) in CA (formerly Computer Associates) Message Queuing (CAM / CAFT) software before 1.11 Build 54_4 on Windows and NetWare, as used in CA Advantage Data Transport, eTrust Admin, certain BrightStor products, certain CleverPath products, and certain Unicenter products, allows remote attackers to execute arbitrary code via a crafted message to TCP port 3104.	unknown 2007-07-25	<a href="#">9.3</a>	<a href="#">CVE-2007-0060</a> <a href="#">ISS</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a> <a href="#">XF</a>

Option  
Computer Associates --  
CleverPath ECM  
Computer Associates --  
Unicenter Management  
Web Servers  
Computer Associates --  
Advantage Data  
Transport  
Computer Associates --  
Unicenter Management  
Microsoft Exchange  
Computer Associates --  
CleverPath OLAP  
Computer Associates --  
BrightStor Portal  
Computer Associates --  
Unicenter Jasmine  
Computer Associates --  
Unicenter Remote Control  
Computer Associates --  
Unicenter Management  
Lotus Note\_Domino  
Computer Associates --  
Unicenter TNG  
Computer Associates --  
Unicenter TNG JPN  
Computer Associates --  
CleverPath Aion  
Computer Associates --  
Unicenter Data Transport  
Option  
Computer Associates --  
eTrust Admin  
Computer Associates --

<p>Unicenter Software Delivery  Computer Associates -- BrightStor SAN Manager  Computer Associates -- Unicenter Network and Systems Management  Computer Associates -- CleverPath Predictive Analysis Server  Computer Associates -- Unicenter Asset Management  Computer Associates -- Unicenter Service Level Management</p>				
<p>Entertainment CMS -- Entertainment CMS</p>	<p>Directory traversal vulnerability in custom.php in Entertainment CMS allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the pagename parameter.</p>	<p>unknown 2007-07-25</p>	<p><a href="#">7.5</a></p>	<p><a href="#">CVE-2007-4008</a> <a href="#">MILWORM</a> <a href="#">BID</a></p>
<p>IBM -- WebSphere Application Server</p>	<p>Multiple unspecified vulnerabilities in IBM WebSphere Application Server (WAS) before Fix Pack 21 (6.0.2.21) have unknown impact and attack vectors, aka (1) PK33799, or (2) a "Potential security exposure" in the Samples component (PK40213).</p>	<p>unknown 2007-07-24</p>	<p><a href="#">9.3</a></p>	<p><a href="#">CVE-2007-3960</a> <a href="#">AIXAPAR</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a></p>
<p>iExpress -- property pro</p>	<p>SQL injection vulnerability in vir_login.asp in iExpress Property Pro allows remote attackers to execute arbitrary SQL commands via the Password parameter. NOTE: the Username parameter is covered by CVE-2006-6029. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.</p>	<p>unknown 2007-07-25</p>	<p><a href="#">7.5</a></p>	<p><a href="#">CVE-2007-3992</a> <a href="#">SECUNIA</a></p>
<p>JBlog -- JBlog</p>	<p>admin/ajoutaut.php in JBlog 1.0 does not require authentication, which allows remote attackers to create</p>	<p>unknown 2007-07-25</p>	<p><a href="#">7.5</a></p>	<p><a href="#">CVE-2007-3974</a> <a href="#">BUGTRAQ</a></p>

	arbitrary accounts via modified mot and droit parameters.			<a href="#">MILWORM BID</a>
junction quest -- image racer	SQL injection vulnerability in SearchResults.asp in ImageRacer 1.0, when WordSearchCrit is enabled, allows remote attackers to execute arbitrary SQL commands via the SearchWord parameter.	unknown 2007-07-25	<a href="#">7.5</a>	<a href="#">CVE-2007-3987</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a> <a href="#">SECUNIA</a> <a href="#">XF</a>
Libvorbis -- libvorbis	libvorbis 1.1.2, and possibly other versions before 1.2.0, allows context-dependent attackers to cause a denial of service and possibly execute arbitrary code via (1) blocksize_0 and blocksize_1 values, which trigger a "heap overwrite" in the _01inverse function in res0.c, (2) an invalid mapping type, which triggers an out-of-bounds read in the vorbis_info_clear function in info.c, and (2) invalid blocksize values that trigger a segmentation fault in the read function in block.c.	unknown 2007-07-26	<a href="#">9.3</a>	<a href="#">CVE-2007-3106</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a>
Libvorbis -- libvorbis	libvorbis 1.1.2, and possibly other versions before 1.2.0, allows context-dependent attackers to cause a denial of service via (1) an invalid mapping type, which triggers an out-of-bounds read in the vorbis_info_clear function in info.c, and (2) invalid blocksize values that trigger a segmentation fault in the read function in block.c.	unknown 2007-07-26	<a href="#">9.3</a>	<a href="#">CVE-2007-4029</a> <a href="#">OTHER-REF</a>
lighttpd -- lighttpd	mod_access.c in lighttpd 1.4.15 ignores trailing / (slash) characters in the URL, which allows remote attackers to bypass url.access-deny settings.	unknown 2007-07-23	<a href="#">8.3</a>	<a href="#">CVE-2007-3949</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a> <a href="#">SECUNIA</a>
Microsoft -- Internet Explorer	Microsoft Windows Explorer (explorer.exe) allows user-assisted remote attackers to cause a denial of service via a certain GIF file, as demonstrated by Art.gif.	unknown 2007-07-24	<a href="#">7.1</a>	<a href="#">CVE-2007-3958</a> <a href="#">MILWORM</a> <a href="#">XF</a>

Norman -- Norman Virus Control	Multiple buffer overflows in Norman Antivirus 5.90 allow remote attackers to execute arbitrary code via a crafted (1) ACE or (2) LZH file, resulting from an "integer cast around."	unknown 2007-07-24	<a href="#">7.5</a>	<a href="#">CVE-2007-3951</a> <a href="#">BUGTRAQ</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a>
Norman -- Normon Antivirus	The OLE2 parsing in Norman Antivirus before 5.91.02 allows remote attackers to bypass the malware detection via a crafted DOC file, resulting from an "integer cast around".	unknown 2007-07-24	<a href="#">7.5</a>	<a href="#">CVE-2007-3952</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a>
Panda -- AdminSecure	Integer overflow in Panda Software AdminSecure allows remote attackers to execute arbitrary code via crafted packets with modified length values to TCP ports 19226 or 19227, resulting in a heap-based buffer overflow.	unknown 2007-07-25	<a href="#">9.3</a>	<a href="#">CVE-2007-3026</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a>
Panda -- Panda AntiVirus	Buffer overflow in Panda Antivirus before 20070720 allows remote attackers to execute arbitrary code via a crafted EXE file, resulting from an "Integer Cast Around."	unknown 2007-07-25	<a href="#">9.3</a>	<a href="#">CVE-2007-3969</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
RCMS Pro -- Rgamescript Pro	PHP remote file inclusion vulnerability in page.php in RCMS Pro RGameScript Pro allows remote attackers to execute arbitrary PHP code via a URL in the id parameter.	unknown 2007-07-25	<a href="#">10.0</a>	<a href="#">CVE-2007-3980</a> <a href="#">MILWORM</a> <a href="#">BID</a>
SWsoft -- Confixx	PHP remote file inclusion vulnerability in admin/business_inc/saveserver.php in SWSoft Confixx Pro 3.3.1 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the thisdir parameter.	unknown 2007-07-25	<a href="#">9.3</a>	<a href="#">CVE-2007-4009</a> <a href="#">MILWORM</a> <a href="#">BID</a>
TeamSpeak -- Web Server	TeamSpeak WebServer 2.0 for Windows does not validate parameter value lengths and does not expire TCP sessions, which allows remote attackers to cause a denial of service (CPU and memory consumption) via long username and	unknown 2007-07-24	<a href="#">7.8</a>	<a href="#">CVE-2007-3956</a> <a href="#">MILWORM</a> <a href="#">BID</a> <a href="#">XF</a>

	password parameters in a request to login.tscmd on TCP port 14534.			
UseBB -- UseBB	Multiple cross-site scripting (XSS) vulnerabilities in UseBB 1.0.7, and possibly other 1.0.x versions, allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO (PHP_SELF) to (1) upgrade-0-2-3.php, (2) upgrade-0-3.php, or (3) upgrade-0-4.php in install/, a different vulnerability than CVE-2005-4193.	unknown 2007-07-25	<a href="#">9.3</a>	<a href="#">CVE-2007-3963</a> <a href="#">BUGTRAQ</a> <a href="#">BID</a>
webSPELL -- webSPELL	Absolute path traversal vulnerability in index.php in Webspell 4.01.02 allows remote attackers to include and execute arbitrary local files via a full pathname in the site parameter. NOTE: some of these details are obtained from third party information.	unknown 2007-07-26	<a href="#">7.5</a>	<a href="#">CVE-2007-4028</a> <a href="#">BUGTRAQ</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
WSN Links -- WSN Links	SQL injection vulnerability in index.php in WSN Links Basic Edition allows remote attackers to execute arbitrary SQL commands via the catid parameter in a displaycat action.	unknown 2007-07-25	<a href="#">7.5</a>	<a href="#">CVE-2007-3981</a> <a href="#">MILWORM</a> <a href="#">BID</a>

[Back to top](#)

### Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Apache -- Tomcat	Cross-site scripting (XSS) vulnerability in SendMailServlet in the examples web application (examples/jsp/mail/sendmail.jsp) in Apache Tomcat 4.0.0 through 4.0.6 and 4.1.0 through 4.1.36 allows remote attackers to inject arbitrary web script or HTML via the From field and possibly other fields, related to generation of error messages.	unknown 2007-07-25	<a href="#">4.3</a>	<a href="#">CVE-2007-3383</a> <a href="#">BUGTRAQ</a> <a href="#">FULLDISC</a> <a href="#">OTHER-REF</a> <a href="#">CERT-VN</a> <a href="#">FRSIRT</a> <a href="#">XF</a>
Areca -- CLI	Buffer overflow in cli32 in Areca CLI 1.72.250 and earlier might allow local users to gain privileges via a long argument. NOTE: this program is not setuid by default, but	unknown 2007-07-26	<a href="#">6.6</a>	<a href="#">CVE-2007-4027</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a>

	there are some usage scenarios in which an administrator might make it setuid.			<a href="#">XF</a>
Aruba -- Mobility Controller	Cross-site scripting (XSS) vulnerability in the login CGI program in Aruba Mobility Controller 2.5.4.18 and earlier, and 2.4.8.6-FIPS and earlier FIPS versions, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2007-07-26	<a href="#">4.3</a>	<a href="#">CVE-2007-4023</a> <a href="#">OTHER-REF</a> <a href="#">SECUNIA</a>
ASP Indir -- cvmatik	Multiple cross-site scripting (XSS) vulnerabilities in cv.asp in Asp cvmatik 1.1 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) Adiniz (Ady), (2) Soyadiniz (Soyady), (3) Ehliyet, (4) Askerlik, and (5) GSM parameters; and possibly other unspecified vectors.	unknown 2007-07-25	<a href="#">4.3</a>	<a href="#">CVE-2007-3991</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a>
Brain Book Software -- AdMan	Multiple cross-site scripting (XSS) vulnerabilities in login.php in AdMan 1.0.20051202 FF 3 patch and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) user and (2) pwd parameters.	unknown 2007-07-26	<a href="#">4.3</a>	<a href="#">CVE-2007-4020</a> <a href="#">OTHER-REF</a>
Brain Book Software -- Software Secure	Multiple cross-site scripting (XSS) vulnerabilities in login.php in Brain Book Software Secure 1.0.20070629 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) user and (2) pwd parameters.	unknown 2007-07-26	<a href="#">4.3</a>	<a href="#">CVE-2007-4021</a> <a href="#">OTHER-REF</a>
bwired -- bwired	Cross-site scripting (XSS) vulnerability in bwired allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: this may be the same as CVE-2007-????.	unknown 2007-07-25	<a href="#">4.3</a>	<a href="#">CVE-2007-3977</a> <a href="#">MILWORM</a>
bwired -- bwired	Session fixation vulnerability in bwired allows remote attackers to hijack web sessions by setting the PHPSESSID parameter.	unknown 2007-07-25	<a href="#">4.3</a>	<a href="#">CVE-2007-3978</a> <a href="#">MILWORM</a>
CA -- etrust Internet Security Suite CA -- CA Anti Virus SDK CA -- AntiSpyware for the Enterprise	arclib.dll before 7.3.0.9 in CA Anti-Virus (formerly eTrust Antivirus) 8 and certain other CA products allows remote attackers to cause a denial of service (infinite loop and loss of antivirus functionality) via an invalid "previous listing chunk number" field in a CHM file.	unknown 2007-07-25	<a href="#">4.3</a>	<a href="#">CVE-2007-3875</a> <a href="#">IDEFENSE</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a>

CA -- Unicenter Network  
Sys management  
CA -- etrust Antivirus  
Gateway  
CA -- BrightStor  
ARCserve Backup for  
Windows  
CA -- Secure Content  
Manager  
CA -- Internet Security  
Suite 2007  
CA -- CA common  
services  
CA -- eTrust Intrusion  
Detection  
CA -- Anti-Virus  
CA -- etrust EZ Antivirus  
CA -- BrightStor  
ARCserve Backup  
CA -- Anti-spyware 2007  
CA -- BrightStor  
Enterprise Backup  
CA -- Anti-Virus for the  
Enterprise  
CA -- BrightStor  
ARCserve Client  
CA -- Protection Suites  
CA -- BrightStor  
ARCserve Client for  
Windows  
CA -- etrust Antivirus  
2007  
CA -- etrust ez armor  
CA -- Threat Manager  
CA -- Antivirus SDK

[SECUNIA](#)

Citrix -- Access Gateway	The Citrix EPA ActiveX control (aka the "endpoint checking control" or CCAOControl Object) before 4.5.0.0 in npCtxCAO.dll in Citrix Access Gateway Standard Edition before 4.5.5 and Advanced Edition before 4.5 HF1 allows remote attackers to download and execute arbitrary programs onto a client system.	unknown 2007-07-25	<a href="#">4.3</a>	<a href="#">CVE-2007-3679</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a>
Citrix -- Advanced Access Control Citrix -- Access Gateway	Unspecified vulnerability in the client components in Citrix Access Gateway Standard Edition before 4.5.5 and Advanced Edition before 4.5 HF1 allows attackers to execute arbitrary code via unspecified vectors.	unknown 2007-07-25	<a href="#">6.8</a>	<a href="#">CVE-2007-4016</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a>
Citrix -- Access Gateway	Citrix Access Gateway Advanced Edition before firmware 4.5.5 allows attackers to redirect users to arbitrary web sites and conduct phishing attacks via unknown vectors.	unknown 2007-07-25	<a href="#">6.8</a>	<a href="#">CVE-2007-4018</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a>
cPanel -- cPanel	Cross-site scripting (XSS) vulnerability in frontend/x/htaccess/changepro.html in cPanel 10.9.1 allows remote attackers to inject arbitrary web script or HTML via the rename parameter.	unknown 2007-07-26	<a href="#">4.3</a>	<a href="#">CVE-2007-4022</a> <a href="#">BUGTRAQ</a> <a href="#">BID</a>
Data Dynamics -- ActiveReports	Absolute path traversal vulnerability in the Data Dynamics ActiveReport (ActiveReports) ActiveX control in actrpt2.dll 2.5 and earlier allows remote attackers to create or overwrite arbitrary files via a full pathname in the first argument to the SaveLayout method.	unknown 2007-07-25	<a href="#">5.8</a>	<a href="#">CVE-2007-3982</a> <a href="#">MILWORM</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
Data Dynamics -- ActiveReports	Absolute path traversal vulnerability in the Data Dynamics DDActiveReports2.ActiveReport.2 (ActiveReports) ActiveX control in apro2.dll in ActiveReports 2.0 Professional	unknown 2007-07-25	<a href="#">6.8</a>	<a href="#">CVE-2007-3983</a> <a href="#">SECUNIA</a>

	Edition 2.5.0.1308 (SP5 RC) allows remote attackers to create or overwrite arbitrary files via a full pathname in an argument to the SaveLayout method. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.			
Elite Forum -- Elite Forum	Cross-site scripting (XSS) vulnerability in index.php in Elite Forum 1.0.0.0 allows remote attackers to inject arbitrary web script or HTML via the title parameter in a ptopic action, a different vulnerability than CVE-2005-3412.	unknown 2007-07-25	<a href="#">4.3</a>	<a href="#">CVE-2007-3975</a> <a href="#">BUGTRAQ</a>
Eset Software -- NOD32 Antivirus	Race condition in ESET NOD32 Antivirus before 2.2289 allows remote attackers to execute arbitrary code via a crafted CAB file, which triggers heap corruption.	unknown 2007-07-25	<a href="#">5.0</a>	<a href="#">CVE-2007-3970</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
Eset Software -- NOD32 Antivirus	Integer overflow in ESET NOD32 Antivirus before 2.2289 allows remote attackers to cause a denial of service (CPU and disk consumption) via a crafted ASPACK packed file, which triggers an infinite loop.	unknown 2007-07-25	<a href="#">5.0</a>	<a href="#">CVE-2007-3971</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
Eset Software -- NOD32 Antivirus	ESET NOD32 Antivirus before 2.2289 allows remote attackers to cause a denial of service via a crafted (1) ASPACK or (2) FSG packed file, which triggers a divide-by-zero error.	unknown 2007-07-25	<a href="#">5.0</a>	<a href="#">CVE-2007-3972</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
FSP -- C Library	Multiple off-by-one errors in fsplib.c in fsplib before 0.8 allow attackers to cause a denial of service via unspecified vectors involving the (1) name and (2) d_name entry	unknown 2007-07-25	<a href="#">5.0</a>	<a href="#">CVE-2006-7221</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a>

	attributes.			
FSP -- C Library	Off-by-one error in the fsp_readdir_r function in fsplib.c in fsplib before 0.9 allows remote attackers to cause a denial of service via a directory entry whose length is exactly MAXNAMELEN, which prevents a terminating null byte from being added.	unknown 2007-07-25	<a href="#">5.0</a>	<a href="#">CVE-2007-3961</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">SECUNIA</a>
FSP -- C Library	Multiple stack-based buffer overflows in fsplib.c in fsplib before 0.9 might allow remote attackers to execute arbitrary code via (1) a long filename that is not properly handled by the fsp_readdir_native function when MAXNAMELEN is greater than 255, or (2) a long d_name directory (dirent) field in the fsp_readdir function.	unknown 2007-07-25	<a href="#">6.4</a>	<a href="#">CVE-2007-3962</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
Gentoo -- NVClock	The set_default_speeds function in backend/backend.c in NVidia NVClock before 0.8b2 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/nvclock temporary file.	unknown 2007-07-25	<a href="#">6.6</a>	<a href="#">CVE-2007-3531</a> <a href="#">OTHER-REF</a> <a href="#">GENTOO</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">SECUNIA</a>
IBM -- AIX	Stack-based buffer overflow in capture in IBM AIX 5.3 SP6 allows remote attackers to execute arbitrary code via a large number of terminal control sequences.	unknown 2007-07-26	<a href="#">6.9</a>	<a href="#">CVE-2007-3333</a> <a href="#">IDEFENSE</a>
IBM -- AIX	pioout in IBM AIX 5.3 SP6 allows local users to execute arbitrary code by specifying a malicious library with the -R (ParseRoutine) command line argument.	unknown 2007-07-26	<a href="#">6.9</a>	<a href="#">CVE-2007-4003</a> <a href="#">IDEFENSE</a>
IBM -- AIX	Buffer overflow in the ftp client in IBM AIX 5.3 SP6 allows local users to execute arbitrary code via unspecified vectors that trigger the overflow in a gets function call. NOTE: the client is setuid root on AIX, so this issue crosses privilege boundaries.	unknown 2007-07-26	<a href="#">6.9</a>	<a href="#">CVE-2007-4004</a> <a href="#">IDEFENSE</a>
iExpress -- Munch Pro	SQL injection vulnerability in Munch Pro allows remote attackers to execute arbitrary SQL commands via the login field to /admin, a different vulnerability than	unknown 2007-07-25	<a href="#">5.0</a>	<a href="#">CVE-2007-3966</a> <a href="#">BUGTRAQ</a> <a href="#">BID</a>

	CVE-2006-5880.			
Ipswitch -- Ipswitch Collaboration Suite Ipswitch -- IMserver	The IM Server (aka IMserve or IMserver) 2.0.5.30 and probably earlier in Ipswitch Instant Messaging before 2.07 in Ipswitch Collaboration Suite (ICS) allows remote attackers to cause a denial of service (daemon crash) via certain data to TCP port 5179 that overwrites a destructor, as reachable by the (1) DoAttachVideoSender, (2) DoAttachVideoReceiver, (3) DoAttachAudioSender, and (4) DoAttachAudioReceiver functions.	unknown 2007-07-24	<a href="#">5.0</a>	<a href="#">CVE-2007-3959</a> <a href="#">IDEFENSE</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a>
ISC -- BIND	The default access control lists (ACL) in ISC BIND 9.4.0, 9.4.1, and 9.5.0a1 through 9.5.0a5 do not set the allow-recursion and allow-query-cache ACLs, which allows remote attackers to make recursive queries and query the cache.	unknown 2007-07-24	<a href="#">5.8</a>	<a href="#">CVE-2007-2925</a> <a href="#">OTHER-REF</a> <a href="#">FRSIRT</a>
ISC -- BIND	ISC BIND 9 through 9.5.0a5 uses a weak random number generator during generation of DNS query ids when answering resolver questions or sending NOTIFY messages to slave name servers, which makes it easier for remote attackers to guess the next query id and perform DNS cache poisoning.	unknown 2007-07-24	<a href="#">6.8</a>	<a href="#">CVE-2007-2926</a> <a href="#">OTHER-REF</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a>
Itaka -- Itaka	Itaka before 0.2.1, when using Authentication mode, allows remote attackers to bypass authentication and obtain sensitive information by downloading screenshots via a direct request for /screenshot.	unknown 2007-07-25	<a href="#">5.0</a>	<a href="#">CVE-2007-3964</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
Jasmine -- CMS	Cross-site scripting (XSS) vulnerability in profile.php in Jasmine CMS 1.0_1 allows remote authenticated users to inject arbitrary web script or HTML via the profile_email parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2007-07-20	<a href="#">4.3</a>	<a href="#">CVE-2007-3941</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">XF</a>
JBlog -- JBlog	Multiple cross-site scripting (XSS) vulnerabilities in JBlog 1.0 allow remote attackers to inject arbitrary web script or	unknown 2007-07-25	<a href="#">6.8</a>	<a href="#">CVE-2007-3973</a> <a href="#">BUGTRAQ</a>

	HTML via the (1) id parameter to (a) index.php, or the (2) search parameter or (3) theme cookie to (b) recherche.php.			<a href="#">MILWORM BID</a>
Kerio -- Kerio MailServer	Unspecified vulnerability in the attachment filter in Kerio MailServer before 6.4.1 has unknown impact and remote attack vectors.	unknown 2007-07-25	<a href="#">5.8</a>	<a href="#">CVE-2007-3993</a> <a href="#">OTHER-REF</a> <a href="#">SECUNIA</a>
lighttpd -- lighttpd	mod_auth (http_auth.c) in lighttpd before 1.4.16 allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors involving (1) a memory leak, (2) use of md5-sess without a cnonce, (3) base64 encoded strings, and (4) trailing whitespace in the Auth-Digest header.	unknown 2007-07-23	<a href="#">6.4</a>	<a href="#">CVE-2007-3946</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a> <a href="#">SECUNIA</a>
lighttpd -- lighttpd	request.c in lighttpd 1.4.15 allows remote attackers to cause a denial of service (daemon crash) by sending an HTTP request with duplicate headers, as demonstrated by a request containing two Location header lines, which results in a segmentation fault.	unknown 2007-07-23	<a href="#">5.8</a>	<a href="#">CVE-2007-3947</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a> <a href="#">SECUNIA</a>
lighttpd -- lighttpd	connections.c in lighttpd before 1.4.16 might accept more connections than the configured maximum, which allows remote attackers to cause a denial of service (failed assertion) via a large number of connection attempts.	unknown 2007-07-23	<a href="#">4.3</a>	<a href="#">CVE-2007-3948</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a> <a href="#">SECUNIA</a>
lighttpd -- lighttpd	lighttpd 1.4.15, when run on 32 bit platforms, allows remote attackers to cause a denial of service (daemon crash) via	unknown	<a href="#">4.3</a>	<a href="#">CVE-2007-3950</a> <a href="#">BUGTRAQ</a>

	unspecified vectors involving the use of incompatible format specifiers in certain debugging messages in the (1) mod_scgi, (2) mod_fastcgi, and (3) mod_webdav modules.	2007-07-23		<a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a> <a href="#">SECUNIA</a>
LinkedIn -- Toolbar	Buffer overflow in the IEToolbar.IEContextMenu.1 ActiveX control in LinkedInIEToolbar.dll in the LinkedIn Toolbar 3.0.2.1098 allows remote attackers to execute arbitrary code via a long second argument (varBrowser argument) to the search method. NOTE: some of these details are obtained from third party information.	unknown 2007-07-24	<a href="#">6.8</a>	<a href="#">CVE-2007-3955</a> <a href="#">MILWORM</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a>
Linux -- RSBAC	Rule Set Based Access Control (RSBAC) before 1.3.5 does not properly use the Linux Kernel Crypto API for the Linux kernel 2.6.x, which allows context-dependent attackers to bypass authentication controls via unspecified vectors, possibly involving User Management password hashing and unchecked function return codes.	unknown 2007-07-23	<a href="#">6.4</a>	<a href="#">CVE-2007-3945</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
Microsoft -- Internet Explorer Mozilla -- SeaMonkey	Argument injection vulnerability in Microsoft Internet Explorer, when running on systems with SeaMonkey installed and certain URIs registered, allows remote attackers to conduct cross-browser scripting attacks and execute arbitrary commands via shell metacharacters in a mailto URI, which are inserted into the command line that is created when invoking SeaMonkey.exe, a related issue to CVE-2007-3670.	unknown 2007-07-24	<a href="#">4.3</a>	<a href="#">CVE-2007-3954</a> <a href="#">OTHER-REF</a> <a href="#">BID</a>
Mike Dubman -- Windows RSH daemon	Stack-based buffer overflow in Mike Dubman Windows RSH daemon (rshd) 1.7 allows remote attackers to execute arbitrary code via a long string to the shell port (514/tcp).	unknown 2007-07-25	<a href="#">5.0</a>	<a href="#">CVE-2007-4005</a> <a href="#">MILWORM</a> <a href="#">BID</a>
Mike Dubman -- Windows RSH daemon	Buffer overflow in Mike Dubman Windows RSH daemon (rshd) 1.7 has unknown impact and remote attack vectors, aka ZD-00000034. NOTE: this information is based upon a vague advisory by a vulnerability information sales	unknown 2007-07-25	<a href="#">6.8</a>	<a href="#">CVE-2007-4006</a> <a href="#">OTHER-REF</a>

	organization that does not coordinate with vendors or release actionable advisories. A CVE has been assigned for tracking purposes, but duplicates with other CVEs are difficult to determine.			
NetArt Media -- Blog System	SQL injection vulnerability in index.php in BlogSite Professional (aka Blog System) 1.x allows remote attackers to execute arbitrary SQL commands via the news_id parameter.	unknown 2007-07-25	<a href="#">6.8</a>	<a href="#">CVE-2007-3979</a> <a href="#">MILWORM</a> <a href="#">BID</a> <a href="#">XF</a>
Nipun Jain -- xserver	Buffer overflow in Nipun Jain xserver 0.1 alpha allows remote attackers to cause a denial of service via a POST request with a long URI.	unknown 2007-07-24	<a href="#">5.0</a>	<a href="#">CVE-2007-3957</a> <a href="#">MILWORM</a>
Norman -- Norman Virus Control	The OLE2 parsing in Norman Antivirus before 5.91.02 allows remote attackers to cause a denial of service via a crafted DOC file that triggers a divide-by-zero error.	unknown 2007-07-24	<a href="#">4.3</a>	<a href="#">CVE-2007-3953</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a>
PHP -- dirLIST	Directory traversal vulnerability in index.php in PHP Directory Lister (dirLIST) before 0.1.1 allows remote attackers to list the contents of a parent directory via a .. (dot dot) in the folder parameter.	unknown 2007-07-25	<a href="#">5.0</a>	<a href="#">CVE-2007-3967</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
PHP -- dirLIST	index.php in dirLIST before 0.1.1 allows remote attackers to list the contents of an excluded folder via a modified URL containing the folder name.	unknown 2007-07-25	<a href="#">5.0</a>	<a href="#">CVE-2007-3968</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
PHP -- PHP	The win32std extension in PHP 5.2.3 does not follow safe_mode and disable_functions restrictions, which allows remote attackers to execute arbitrary commands via the win_shell_execute function.	unknown 2007-07-25	<a href="#">6.8</a>	<a href="#">CVE-2007-4010</a> <a href="#">MILWORM</a> <a href="#">BID</a>
QuickerSite -- QuickerSite	Cross-site scripting (XSS) vulnerability in default.asp in QuickerSite 1.7.2 allows remote attackers to inject arbitrary web script or HTML via the svalue parameter in a search action. NOTE: some of these details are obtained from third party information.	unknown 2007-07-20	<a href="#">4.3</a>	<a href="#">CVE-2007-3940</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">XF</a>

Secure Computing -- SecurityReporter	Directory traversal vulnerability in file.cgi in Secure Computing SecurityReporter (aka Network Security Analyzer) 4.6.3 allows remote attackers to download arbitrary files via a .. (dot dot) in the name parameter.	unknown 2007-07-25	<a href="#">5.0</a>	<a href="#">CVE-2007-3985</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
Secure Computing -- SecurityReporter	file.cgi in Secure Computing SecurityReporter (aka Network Security Analyzer) 4.6.3 allows remote attackers to bypass authentication via a name parameter that specifies the eventcache directory and a non-GIF file, which causes the \$dontvalidate variable to be set to true. NOTE: a separate traversal vulnerability could be leveraged to download arbitrary files.	unknown 2007-07-25	<a href="#">5.0</a>	<a href="#">CVE-2007-3986</a> <a href="#">BUGTRAQ</a> <a href="#">OTHER-REF</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
Simple Machines -- Simple Machines Forum	<b>** DISPUTED **</b> Directory traversal vulnerability in index.php in Simple Machines Forum (SMF) 1.1.3 allows remote attackers to include local files via unspecified vectors related to the sourcedir parameter or the actionArray hash. NOTE: CVE and multiple third parties dispute this vulnerability because both sourcedir and actionArray are defined before use.	unknown 2007-07-20	<a href="#">5.8</a>	<a href="#">CVE-2007-3942</a> <a href="#">BUGTRAQ</a> <a href="#">BUGTRAQ</a> <a href="#">XF</a>
Sun -- Java System Application Server	Unspecified vulnerability in Sun Java System (SJS) Application Server 8.1 through 9.0 before 20070724 on Windows allows remote attackers to obtain JSP source code via unspecified vectors.	unknown 2007-07-26	<a href="#">4.3</a>	<a href="#">CVE-2007-4025</a> <a href="#">SUNALERT</a> <a href="#">SECUNIA</a>
Telaxus LLC -- epesi	epesi framework before 0.8.6 does not properly verify file extensions, which allows remote attackers to upload and execute arbitrary PHP code via unspecified vectors involving the gallery images upload feature. NOTE: some of these details are obtained from third party information.	unknown 2007-07-26	<a href="#">6.8</a>	<a href="#">CVE-2007-4026</a> <a href="#">OTHER-REF</a> <a href="#">SECUNIA</a>
ufmod -- ufmod Xm player Library	Unspecified vulnerability in uFMOD before 1.2.5 has unknown impact and attack vectors, possibly related to malformed files, and possibly an integer signedness error for relative note instruments.	unknown 2007-07-25	<a href="#">6.8</a>	<a href="#">CVE-2007-3965</a> <a href="#">OTHER-REF</a> <a href="#">BID</a> <a href="#">SECUNIA</a>

Virtual Hosting Control System -- Virtual Hosting Control System	Session fixation vulnerability in Virtual Hosting Control System (VHCS) 2.4.7.1 and earlier allows remote attackers to hijack web sessions by setting the PHPSESSID parameter.	unknown 2007-07-25	<a href="#">6.0</a>	<a href="#">CVE-2007-3988</a> <a href="#">BUGTRAQ</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
W1L3D4 -- Philboard	Cross-site scripting (XSS) vulnerability in W1L3D4_aramasonuc.asp in W1L3D4 Philboard 0.3 allows remote attackers to inject arbitrary web script or HTML via the searchterms parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2007-07-26	<a href="#">4.3</a>	<a href="#">CVE-2007-4024</a> <a href="#">SECUNIA</a>
WordPress -- Blix WordPress -- BlixKrieg WordPress -- Blixed	Cross-site scripting (XSS) vulnerability in a certain index.php installation script related to the (1) Blix 0.9.1, (2) Blixed 1.0, and (3) BlixKrieg (Blix Krieg) 2.2 themes for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter, possibly a related issue to CVE-2007-2757. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2007-07-25	<a href="#">4.3</a>	<a href="#">CVE-2007-4014</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">SECUNIA</a> <a href="#">SECUNIA</a> <a href="#">XF</a> <a href="#">XF</a> <a href="#">XF</a>
Zenturi -- Zenturi ProgramChecker	Buffer overflow in a certain ActiveX control in the NixonMyPrograms class in sasatl.dll 1.5.0.531 in Zenturi ProgramChecker allows remote attackers to execute arbitrary code via a long argument to the Scan method. NOTE: this is probably a different issue than CVE-2007-2987.	unknown 2007-07-25	<a href="#">6.4</a>	<a href="#">CVE-2007-3984</a> <a href="#">MILWORM</a> <a href="#">BID</a>

[Back to top](#)

### Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
---------------------------	-------------	----------------------	------------	---------------------

[Back to top](#)

**Last updated July 30, 2007**