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
BadBlue -- BadBlue	BadBlue 2.72 Personal Edition stores multiple programs in the web document root with insufficient access control, which allows remote attackers to (1) cause a denial of service via multiple invocations of uninst.exe, and have an unknown impact via (2) badblue.exe and (3) dyndns.exe. NOTE: this can be leveraged for arbitrary remote code execution in conjunction with CVE-2007-6378.	unknown 2008-04-28	7.5	CVE-2008-2003 BUGTRAQ
IBM -- DB2 Server	Unspecified vulnerability in the ADMIN_SP_C2 procedure in IBM DB2 8 before FP16, 9.1 before FP4a, and 9.5 before FP1 allows remote authenticated users to execute arbitrary code via unknown vectors. NOTE: the ADMIN_SP_C issue is already covered by CVE-2008-0699.	unknown 2008-04-28	9.0	CVE-2008-1997 BUGTRAQ AIXAPAR
IBM -- DB2	The NNSTAT (aka SYSPROC.NNSTAT) procedure in IBM DB2 8 before FP16, 9.1	unknown	8.5	CVE-2008-1998 BUGTRAQ

	before FP4a, and 9.5 before FP1 on Windows allows remote authenticated users to overwrite arbitrary files via the log file parameter.	2008-04-28		AIXAPAR AIXAPAR AIXAPAR
Motorola -- Surfboard	Multiple cross-site request forgery (CSRF) vulnerabilities on Motorola Surfboard with software SB5100-2.3.3.0-SCM00-NOSH allow remote attackers to (1) cause a denial of service (device reboot) via the "Restart Cable Modem" value in the BUTTON_INPUT parameter to configdata.html, and (2) cause a denial of service (hard reset) via the "Reset All Defaults" value in the BUTTON_INPUT parameter to configdata.html.	unknown 2008-04-28	7.8	CVE-2008-2002 BUGTRAQ OTHER-REF
WordPress -- WordPress	The cookie authentication method in WordPress 2.5 relies on a hash of a concatenated string containing USERNAME and EXPIRY_TIME, which allows remote attackers to forge cookies by registering a username that results in the same concatenated string, as demonstrated by registering usernames beginning with "admin" to obtain administrator privileges, aka a "cryptographic splicing" issue. NOTE: this vulnerability exists because of an incomplete fix for CVE-2007-6013.	unknown 2008-04-28	7.5	CVE-2008-1930 OTHER-REF OTHER-REF BID

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Apple -- Safari	Apple Safari 3.1.1 allows remote attackers to spoof the address bar by placing many "invisible" characters in the userinfo subcomponent of the authority component of the URL (aka the user field), as demonstrated by %E3%80%80 sequences.	unknown 2008-04-28	5.0	CVE-2008-1999 BUGTRAQ OTHER-REF FRSIRT SECUNIA XF
Apple -- Safari	Unspecified vulnerability in Apple Safari 3.1.1 allows remote attackers to cause a denial of service (application crash) via JavaScript code that calls document.write in an infinite loop.	unknown 2008-04-28	4.3	CVE-2008-2000 BUGTRAQ OTHER-REF FRSIRT XF
Apple -- Safari	Apple Safari 3.1.1 allows remote attackers to cause a denial of service	unknown 2008-04-28	4.3	CVE-2008-2001 BUGTRAQ

	(application crash) via a file:///%E2 link that triggers an out-of-bounds access, possibly due to a NULL pointer dereference.			OTHER-REF FRSIRT XF
Blender -- Blender	Multiple unspecified vulnerabilities in Blender have unknown impact and attack vectors, related to "temporary file issues."	unknown 2008-04-28	4.6	CVE-2008-1103 SUSE BID
Cerulean Studios -- Trillian	Buffer overflow in the Display Names message feature in Cerulean Studios Trillian Basic and Pro 3.1.9.0 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a long nickname in an MSN protocol message.	unknown 2008-04-29	6.8	CVE-2008-2008 BUGTRAQ BID FRSIRT SECUNIA
LICQ -- LICQ	licq before 1.3.6 allows remote attackers to cause a denial of service (file-descriptor exhaustion and application crash) via a large number of connections.	unknown 2008-04-28	5.0	CVE-2008-1996 BUGTRAQ BUGTRAQ BUGTRAQ MLIST OTHER-REF OTHER-REF SUSE BID
ltsp -- linux_terminal_server_project	ldm in Linux Terminal Server Project (LTSP) 0.99 and 2 pass the -ac option to the X server on each LTSP client, which allows remote attackers to connect to this server via TCP port 6006 (aka display	unknown 2008-04-29	4.8	CVE-2008-1293 MLIST MLIST OTHER-REF DEBIAN BID

Back to top

There were no low vulnerabilities recorded this week.