JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Maintaining Scanners

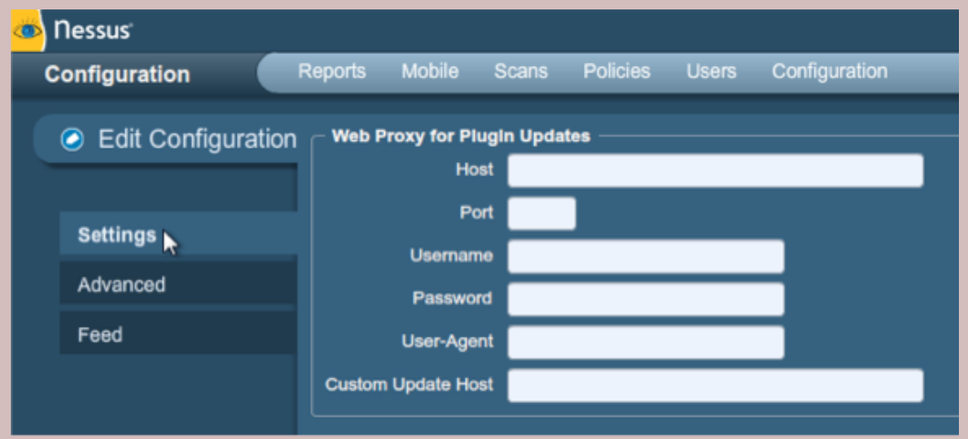
VULNERABILITY MANAGEMENT

Maintaining Scanners

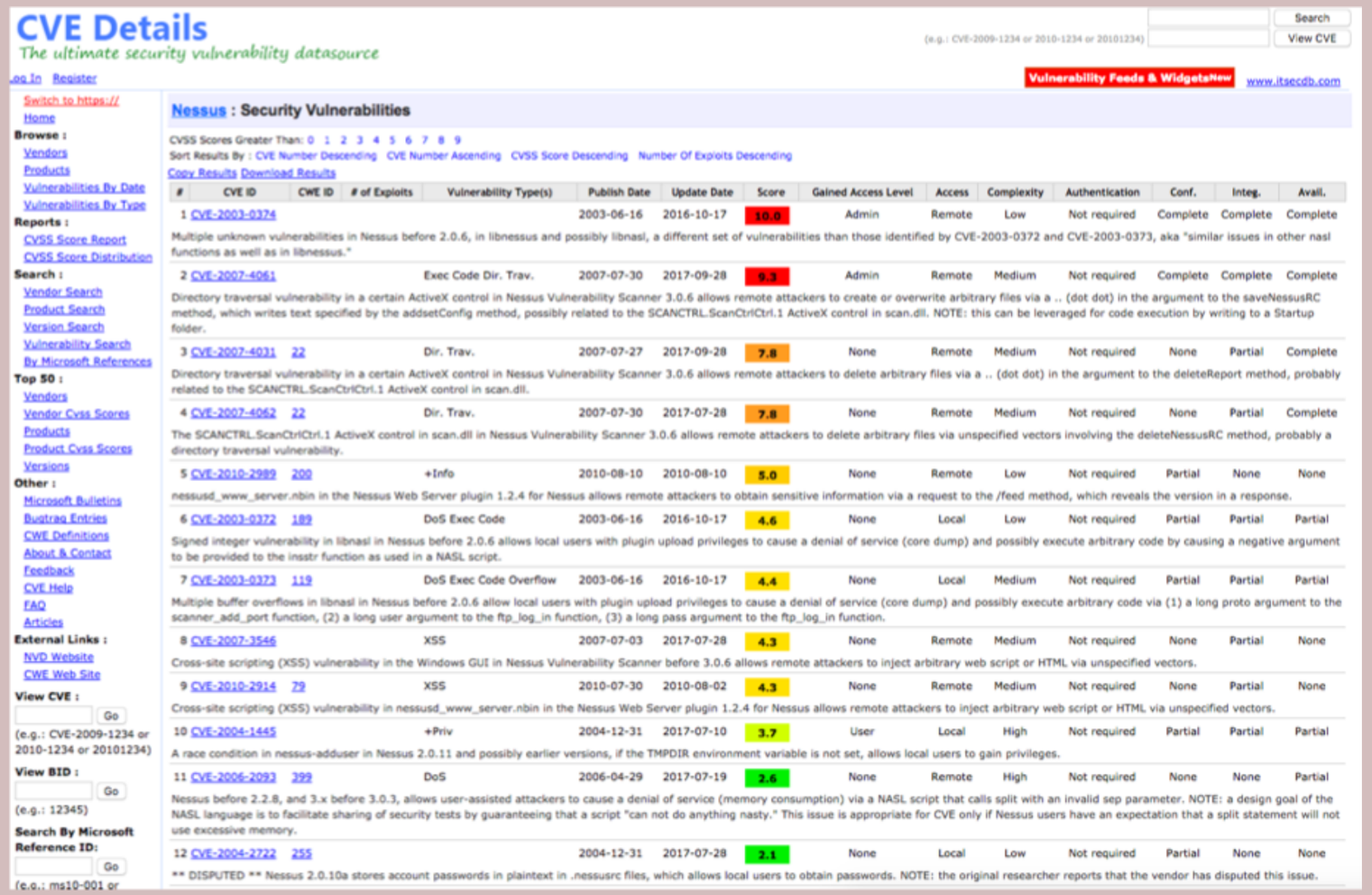
- Vulnerability management tools are vulnerable to vulnerabilities themselves!
- You should always update the tools and its plug-ins/signatures before use
- This can be automated, as well, but check to verify the update has occurred before use

Updating Scanners

- Regular patching is critical to a secure scanner
- Implements bug fixes
- Feature enhancements
- Improves scan quality



Nessus Scanner Vulnerabilities



CVE Details
The ultimate security vulnerability datasource

Search | View CVE (e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In | Register

Vulnerability Feeds & WidgetsNew | www.itsecdb.com

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE : Go (e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
View BID : Go (e.g.: 12345)
Search By Microsoft Reference ID: Go (e.g.: ms10-001 or

Nessus : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending | CVE Number Ascending | CVSS Score Descending | Number Of Exploits Descending
Copy Results | Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2003-0374				2003-06-16	2016-10-17	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
	Multiple unknown vulnerabilities in Nessus before 2.0.6, in libnessus and possibly libnasl, a different set of vulnerabilities than those identified by CVE-2003-0372 and CVE-2003-0373, aka "similar issues in other nasl functions as well as in libnessus."													
2	CVE-2007-4061			Exec Code Dir. Trav.	2007-07-30	2017-09-28	9.3	Admin	Remote	Medium	Not required	Complete	Complete	Complete
	Directory traversal vulnerability in a certain ActiveX control in Nessus Vulnerability Scanner 3.0.6 allows remote attackers to create or overwrite arbitrary files via a .. (dot dot) in the argument to the saveNessusRC method, which writes text specified by the addsetConfig method, possibly related to the SCANCTRL.ScanCtrlCtrl.1 ActiveX control in scan.dll. NOTE: this can be leveraged for code execution by writing to a Startup folder.													
3	CVE-2007-4031	22		Dir. Trav.	2007-07-27	2017-09-28	7.8	None	Remote	Medium	Not required	None	Partial	Complete
	Directory traversal vulnerability in a certain ActiveX control in Nessus Vulnerability Scanner 3.0.6 allows remote attackers to delete arbitrary files via a .. (dot dot) in the argument to the deleteReport method, probably related to the SCANCTRL.ScanCtrlCtrl.1 ActiveX control in scan.dll.													
4	CVE-2007-4062	22		Dir. Trav.	2007-07-30	2017-07-28	7.8	None	Remote	Medium	Not required	None	Partial	Complete
	The SCANCTRL.ScanCtrlCtrl.1 ActiveX control in scan.dll in Nessus Vulnerability Scanner 3.0.6 allows remote attackers to delete arbitrary files via unspecified vectors involving the deleteNessusRC method, probably a directory traversal vulnerability.													
5	CVE-2010-2989	200		+Info	2010-08-10	2010-08-10	5.0	None	Remote	Low	Not required	Partial	None	None
	nessusd_www_server.nbin in the Nessus Web Server plugin 1.2.4 for Nessus allows remote attackers to obtain sensitive information via a request to the /feed method, which reveals the version in a response.													
6	CVE-2003-0372	189		DoS Exec Code	2003-06-16	2016-10-17	4.6	None	Local	Low	Not required	Partial	Partial	Partial
	Signed integer vulnerability in libnasl in Nessus before 2.0.6 allows local users with plugin upload privileges to cause a denial of service (core dump) and possibly execute arbitrary code by causing a negative argument to be provided to the insstr function as used in a NASL script.													
7	CVE-2003-0373	119		DoS Exec Code Overflow	2003-06-16	2016-10-17	4.4	None	Local	Medium	Not required	Partial	Partial	Partial
	Multiple buffer overflows in libnasl in Nessus before 2.0.6 allow local users with plugin upload privileges to cause a denial of service (core dump) and possibly execute arbitrary code via (1) a long proto argument to the scanner_add_port function, (2) a long user argument to the ftp_log_in function, (3) a long pass argument to the ftp_log_in function.													
8	CVE-2007-3546			XSS	2007-07-03	2017-07-28	4.3	None	Remote	Medium	Not required	None	Partial	None
	Cross-site scripting (XSS) vulnerability in the Windows GUI in Nessus Vulnerability Scanner before 3.0.6 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.													
9	CVE-2010-2914	79		XSS	2010-07-30	2010-08-02	4.3	None	Remote	Medium	Not required	None	Partial	None
	Cross-site scripting (XSS) vulnerability in nessusd_www_server.nbin in the Nessus Web Server plugin 1.2.4 for Nessus allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.													
10	CVE-2004-1445			+Priv	2004-12-31	2017-07-10	3.7	User	Local	High	Not required	Partial	Partial	Partial
	A race condition in nessus-adduser in Nessus 2.0.11 and possibly earlier versions, if the TMPDIR environment variable is not set, allows local users to gain privileges.													
11	CVE-2006-2093	399		DoS	2006-04-29	2017-07-19	2.6	None	Remote	High	Not required	None	None	Partial
	Nessus before 2.2.8, and 3.x before 3.0.3, allows user-assisted attackers to cause a denial of service (memory consumption) via a NASL script that calls split with an invalid sep parameter. NOTE: a design goal of the NASL language is to facilitate sharing of security tests by guaranteeing that a script "can not do anything nasty." This issue is appropriate for CVE only if Nessus users have an expectation that a split statement will not use excessive memory.													
12	CVE-2004-2722	255			2004-12-31	2017-07-28	2.1	None	Local	Low	Not required	Partial	None	None
	** DISPUTED ** Nessus 2.0.10a stores account passwords in plaintext in .nessusrc files, which allows local users to obtain passwords. NOTE: the original researcher reports that the vendor has disputed this issue.													

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Updating Plug-ins

- Plug-ins can be automatically set to update daily
- Provides signatures for latest vulnerabilities