

NESSUS PROFESSIONAL

THE DE FACTO INDUSTRY STANDARD FOR VULNERABILITY ASSESSMENT

Scarce resources, limited time, a constantly changing attack surface – it's difficult for security practitioners on the front lines to keep pace with attackers. You need a fast, easy way to proactively find and fix vulnerabilities.

Nessus® Professional automates point-in-time assessments to help quickly identify and fix vulnerabilities, including software flaws, missing patches, malware, and misconfigurations, across a variety of operating systems, devices and applications

NESSUS IS #1IN VULNERABILITY ASSESSMENT

#1 in Accuracy

Nessus has the industry's lowest false positive rate with sixsigma accuracy (measured at .32 defects per 1 million scans).

#1 in Coverage

Nessus has the deepest and broadest coverage with more than 130,000 plugins, coverage for more than 50,000 CVE and over 100 new plugins released weekly within 24 hours of vulnerability disclosure.

#1 in Adoption

Nessus is trusted by more than 30,000 organizations globally, including 2 million downloads. 50% of the Fortune 500 and more than 30% of the Global 2000 rely on Nessus technology.

BREADTH AND DEPTH OF COVERAGE

Tenable Research works closely with the security community to discover new vulnerabilities (we have discovered more than 100 zero-day vulnerabilities over the past three years) and provide insights to help organizations mature their vulnerability assessment practices. We build this intelligence into Nessus through plugins to help take the guesswork out of vulnerability assessment – without requiring you to be an expert – for more accurate, comprehensive vulnerability assessment.

AUTOMATIC PLUGIN UPDATES: SHRINK THE TIME TO ASSESS AND REMEDIATE

With more than 130,000 plugins automatically updating in real-time, Nessus helps you save valuable time to assess, research and remediate issues.

- Custom plugins allow you to create specific checks to assess the security of applications unique to your organization.
- Custom audit files help you verify your organization's configuration requirements and compliance standards.

			P	≙ localhost	Ċ			1
essus 🔊 👘	Soans Settings						•	glen 🤇
	CRTCAL Bash	Remote Code Execut	ion (Shellshock)		<	> Plugin Details		
My Scans						Severity:	Critical	
All Scens	Description					ID:	77823	
Treah		ning a version of Bash that is stern, an attacker could remot		environment variable manipulation. Depending on the		Version:	1.7	
	conguestor or the sy		ay execute a carriery coole.			Type	local	
						Family:	Gain a shell remotely	
Policies	Solution Update Bash.					Published:	September 24, 2014	
	Update Bash.					Modifect	October 28, 2014	
Plugin Rules								
Customized Reports	See Also					Bisk Informatic		
§: Boarnes	http://www.nesous.org/vms-esoc/2014/rg/ht50 http://www.nesous.org/v74/rg/ht50					Pisk information		
	https://www.invisibilitytes.cs/2014/02/tr/					Risk Factor: Onlical		
					CVSS Base Score: 10.0			
	Owtput				CVSS Temporal Score: 8.7			
	Output				CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C			
	Messus was able to set the THEM environment variable used in an SEE					CVSS Temporal Vector: CVSS24E:ND/RL:OF/RC:C IAVM Seventy: I		
	connection to :							
	() (ij) /usr/bin/id > /usp/sessas.1430341545							
	and read the output from the file :					Vulnerability Information		
	sh -c 'bash -c '\''cat /tmp/nessus.1430947545'<-j# sh -c 'bash -c '\''cat /tmp/nessus.1430947545'\					CPE: ope/agnutbash Exploit Available: tue		
	uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel) context=root;system_riuncoofined_t;SystemLav- SystemDich							
	pyramusja Enter Hemans has attempted to remove the file /tmp/ceesus.110047345 Port - Hoom				Exploit Ease: Exploits are graliable			
					Patch Pub Date: September 24, 2014			
					Vulnerability Pub Date: September 24, 2014			
	22 / top / ssh	172.26.16.211						
						Exploitable Wit	th	
						Metasplot (Pure-PTPd External Authentication Bash Environment Variable Code Injection)		
	Bessue was abl	e to set the TERM eavi	set the TERM environment variable used in an SSE					10
	connection to (Core Impact		
	() [17]2 /usr/bin/id > /tmp/nessus.1430947693							
	and read the output from the file :					Reference Information		
	uid=1003(seo) gid=100(secs) group=100(usecs),9(root),1(bis),3(sys),5(tty),16(dislout),22(utmp),33(video),42(trusted),65(sshd),111(suse- nec),1000(seanner),1001(Meo_Noot)					EDB-ID: 34766	ED8-ID: 34766, 34765 BID: 70103 OSVDB: 112004	
	Note: Nessus has attempted to remove the file /tmp/nessus.1430947693					OSVDB: 11200		
	Port -	Petr. Rosts 22 / sur / etc 172 2017 48				WWA: 2014-A-0142 CVE: CVE-2014-6271		
	22 / top / sels							

Each automatic **Plugin** update provides you with a simple set of remediation actions, and a fast and easy way to see if your systems are vulnerable.

Insights through threat intelligence feeds

Gain insight into potential malware running on hosts throughout your environment via seamless integration with multiple commercial threat intelligence feeds.

LEVERAGE THE POWER OF PREDICTIVE PRIORITIZATION

Take advantage of Tenable's Vulnerability Priority Rating (VPR) to help you zero in on the vulnerabilities that pose the greatest risk. VPR combines Tenable-collected vulnerability data with third-party vulnerability and threat data and analyzes them together with the advanced data science algorithm developed by Tenable Research.

Broad, deep visibility into vulnerabilities

Get broad and deep visibility into vulnerabilities with every assessment. Nessus offers coverage for over 47,000 unique IT assets, including:

- Network devices (e.g., Cisco, Juniper, HP, F5 and SonicWall)
- MobileIron and VMware AirWatch to assess mobile devices for vulnerabilities against policies
- Operating systems (e.g., Windows, MacOS, and Linux)
- Applications ranging from small driver update utilities to complex Office productivity suites

"Well-organized interface which classifies plugins in a neat, structured manner."

- Nessus user

CONSULTANTS LOVE NESSUS

Nessus is ideal for security consultants because it offers:

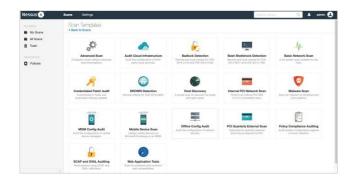
- Unlimited assessments No limit to the number of IPs or assessments.
- Easily transferable license Quickly and easily transfer your license between computers.
- Configurable reports Easily customize reports with client name and logo. Email directly to the client after every assessment.

EASE OF USE

Built for security practitioners, by security practitioners, Nessus was created with the single focus of providing an intuitive experience for security pros on the front lines to find and fix vulnerabilities, faster and more confidently.

Quickly see vulnerabilities with pre-built policies and templates

Out-of-the-box, pre-configured templates for IT and mobile assets, including configuration audits, help you quickly understand where you have vulnerabilities.



More than 450 compliance and configuration templates allow you to audit configuration compliance against CIS benchmarks and other best practices.

Intelligent vulnerability assessment with Live Results

Live Results performs intelligent vulnerability assessment in offline mode with every plugin update – without having to run a scan. Just log in and see the results of potential vulnerabilities based on your scan history. With a click of a button, you can run a scan to validate the presence of the vulnerability, creating a faster, more efficient process for assessing, prioritizing and remediating issues.

Configure reports easily

Create reports based on customized views (e.g., specific vulnerability types, vulnerabilities by host/plugin, by team/ client) – in a variety of formats (HTML, CSV and Nessus XML).

Laser focus with Grouped View

Similar issues or categories of vulnerabilities are grouped together and presented in one thread. Snoozing allows users to select issues to disappear from view for a specified period of time. This helps with prioritization, allowing you to focus only on the issues you are working on at a given time.

ADVANCED SUPPORT AVAILABLE

Nessus Professional customers can access email, portal, chat and phone support 24 hours a day, 365 days a year with a subscription to the Advanced level of technical support. This will also help ensure faster response times and resolution. Full details about support plans can be found <u>here</u>.

ABOUT TENABLE

Tenable[®], Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus[®], Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at <u>www.tenable.com</u>.

For More Information: Please visit <u>tenable.com</u> Contact Us: Please email us at <u>sales@tenable.com</u> or visit <u>tenable.com/contact</u>



YRIGHT 2021 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE, TENABLE IO, TENABLE NETWORK SECURITY, NESSUS, CURITYCENTER, SECURITYCENTER CONTINUOUS VIE WAND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, C. TENABLE.SC, TENABLE.OT, LUMIN, INDEGY ASSURE, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. L. DIYHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.

Data Sheet / Nessus / 040921