

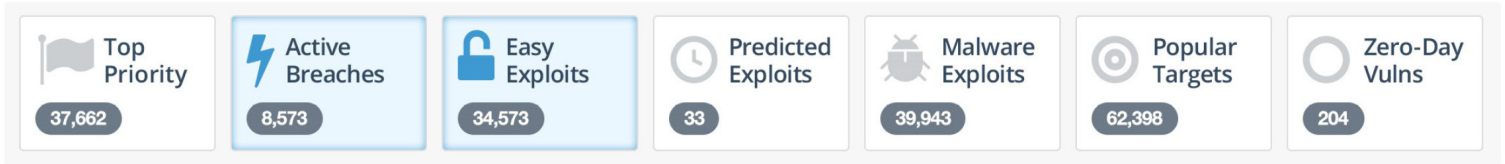


Why Your Organization Needs AVA?

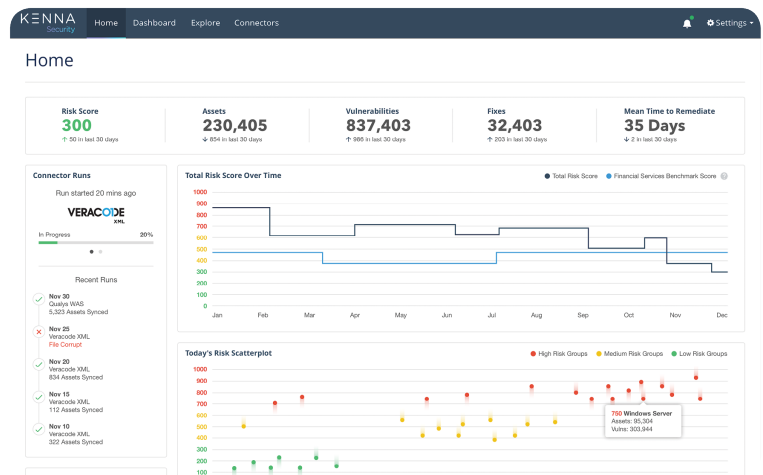
- ✓ **Easy to Subscribe and Initiate**
Security experts at MCNC make setup and use a breeze
- ✓ **Know Your Security Risk Score**
Advanced technology and real-world data that serves as a compass for all risk operations
- ✓ **Smart Remediation**
Actionable measurements that guide remediation efforts and resource allocation
- ✓ **Dashboard & Reporting**
Customized and fully automated workflow that produces essential cyber risk reporting and evaluation
- ✓ **Low-Cost High Impact**
A comprehensive vulnerability management solution at a fraction of the cost

Contact us for a quote at **(919) 248-1999** or via email at **info@mcnc.org**. Visit us online at **www.mcnc.org/our-solutions/security/active-vulnerability-analysis** to get your Active Vulnerability Access solution today.

MCNC's AVA service scans your network for vulnerabilities, calculates risk, and prioritizes which issues to address. These risk scores use machine learning to discover which vulnerabilities are actively being used in successful breaches, how easily breached a vulnerability is, how popular a specific exploit is, and if malware exists to exploit a specific vulnerability.



Score	Name	Asset	Created
100 / 100	CVE-2012-0013 Incomplete blacklist vulnerability in the Windows Packager configuration in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted ClickOnce application in a Microsoft Office document, related to .application files, aka "Assembly Execution Vulnerability."	vinay-24-64.testing.compliance.vuln.qa.qualys.com SLP servers servers DMZ	11 months ago
100 / 100	CVE-2012-1823 sapi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by plusing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'o' case.	vinay-24-64.testing.compliance.vuln.qa.qualys.com SLP servers servers DMZ	11 months ago
100 / 100	CVE-2012-1823 Stack-based buffer overflow in the setDIR() function in the Abstract Window Toolkit (AWT) in Java Runtime Environment (JRE) in Sun Java SE in JDK and JRE 5.0 before Update 22, JDK and JRE 6 before Update 17, SDK and JRE 1.3.x before 1.3.1_27, and SDK and JRE 1.4.x before 1.4.2_24 allows remote attackers to execute arbitrary code via a crafted argument, aka Bug id 6872557.	vinay-24-64.testing.compliance.vuln.qa.qualys.com SLP servers servers DMZ	11 months ago



✓ You access your prioritized vulnerability data and continuously updated risk scores in a customized web portal.

“ Active Vulnerability Analysis is very helpful information and we are already turning it into actionable items for us to improve our security posture. Thank you for your support on this new resource. It is already proving to be a good asset. ”

- MCNC K-12 Client

Contact us for a quote at (919) 248-1999 or via email at info@mcnc.org. Visit us online at www.mcnc.org/our-solutions/security/active-vulnerability-analysis to get your Active Vulnerability Access solution today.