THREATDEFEND® FEATURE HIGHLIGHT: VULNERABILITY SIMULATION

OVERVIEW

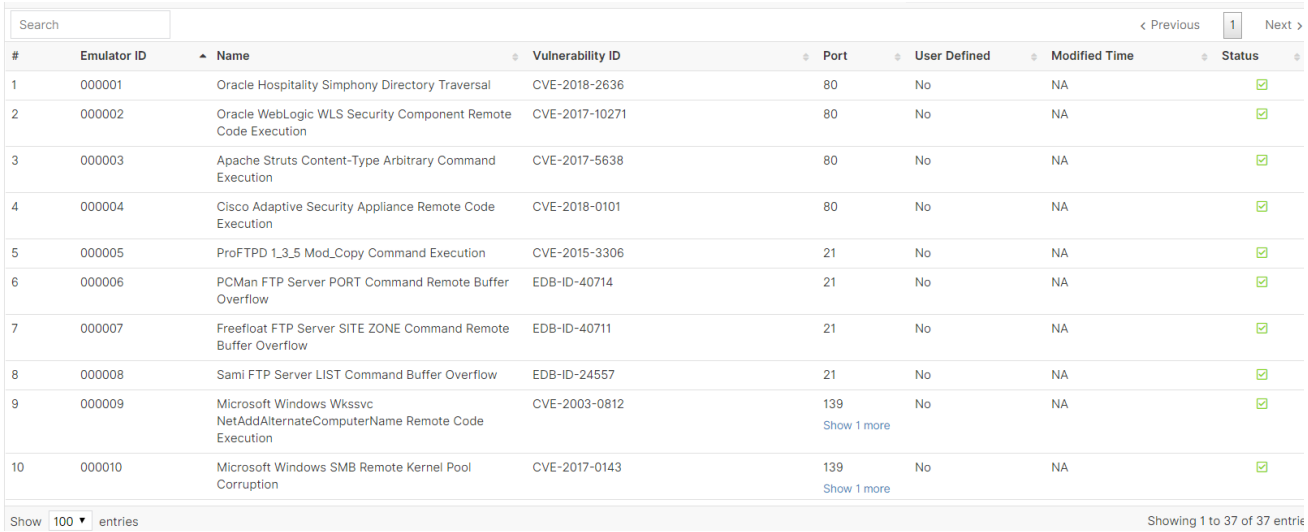
Organizations can configure the Attivo Networks® BOTsink® appliance to simulate known vulnerabilities, giving highly accurate alerts if an attacker attempts to leverage one against the organization. This form of simulation responds to an attacker's effort as if it was vulnerable without actually compromising the target host or allowing the attacker to expand their footprint.

This functionality is especially useful for organizations that are concerned with specific vulnerabilities and want a clear indication if an attacker is trying to use them.

VULNERABILITY SIMULATION

Every year, thousands of new vulnerabilities are documented, catalogued, and published in several repositories, such as MITRE's CVE database and the Exploit Database, giving organizations the ability to recognize them and take the appropriate actions to defend against them. These publications document the parameters of each attack and how a vulnerable system service would respond.

The Attivo Networks vulnerability simulation feature includes a library of known vulnerabilities, out of the box, that can identify any attempt to exploit them and respond accordingly, leading an attacker to believe the target system is vulnerable and their attack was a success. While an attacker may, at some point, realize that the attack did not work as it appeared to, the BOTsink appliance will have already identified the attempt and alerted the information security team to the attacker's presence.



Search ‹ Previous 1 Next ›

#	Emulator ID	Name	Vulnerability ID	Port	User Defined	Modified Time	Status
1	000001	Oracle Hospitality Simphony Directory Traversal	CVE-2018-2636	80	No	NA	☑
2	000002	Oracle WebLogic WLS Security Component Remote Code Execution	CVE-2017-10271	80	No	NA	☑
3	000003	Apache Struts Content-Type Arbitrary Command Execution	CVE-2017-5638	80	No	NA	☑
4	000004	Cisco Adaptive Security Appliance Remote Code Execution	CVE-2018-0101	80	No	NA	☑
5	000005	ProFTPD 1_3_5 Mod_Copy Command Execution	CVE-2015-3306	21	No	NA	☑
6	000006	PCMan FTP Server PORT Command Remote Buffer Overflow	EDB-ID-40714	21	No	NA	☑
7	000007	Freefloat FTP Server SITE ZONE Command Remote Buffer Overflow	EDB-ID-40711	21	No	NA	☑
8	000008	Sami FTP Server LIST Command Buffer Overflow	EDB-ID-24557	21	No	NA	☑
9	000009	Microsoft Windows Wkssvc NetAddAlternateComputerName Remote Code Execution	CVE-2003-0812	139 Show 1 more	No	NA	☑
10	000010	Microsoft Windows SMB Remote Kernel Pool Corruption	CVE-2017-0143	139 Show 1 more	No	NA	☑

Show 100 entries Showing 1 to 37 of 37 entrie

PRACTICAL USE

Organizations that wish to add environmentally relevant vulnerabilities can leverage published sources to expand the onboard library. Most sources utilize common formats that are easy to parse and import into the BOTsink appliance.

The BOTsink appliance can accept new and updated vulnerability information and add it to the local database. An organization can easily detect efforts to exploit the vulnerabilities they are most concerned with while discounting ones that aren't relevant to their environment.

The ability to customize simulations provides organizations the ability to most efficiently use their Infosec resources and improve their overall security posture.

AVALIABILITY

The Attivo Networks Vulnerability Simulator is available across the entire BOTsink solution range, including physical, virtual, and Cloud instances.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in deception technology, provides an active defense for early detection, forensics, and automated incident response to in-network attacks. The Attivo ThreatDefend™ Deception Platform provides a comprehensive and customer-proven platform for proactive security and accurate threat detection within user networks, data centers, clouds, and a wide variety of specialized attack surfaces. The portfolio includes expansive network, endpoint, application, and data deceptions designed to efficiently misdirect and reveal attacks from all threat vectors. Advanced machine-learning makes preparation, deployment, and operations fast and simple to operate for organizations of all sizes. Comprehensive attack analysis and forensics provide actionable alerts, and native integrations automate the blocking, quarantine, and threat hunting of attacks for accelerated incident response. The company has won over 70 awards for its technology innovation and leadership.