# Tenable Products Plugin Families

July 29, 2016

(Revision 7)

# Table of Contents

# Introduction

This document describes Tenable Network Security's product plugin families for Nessus, Log Correlation Engine (LCE), and the Passive Vulnerability Scanner (PVS). Please email any comments and questions to support@tenable.com.

A basic understanding of the product in use is assumed.

Vulnerabilities in hosts on your network provide the possibility of data compromise. Tenable Nessus, PVS, and LCE gather complementary security data that can be correlated with Tenable SecurityCenter Continuous View for a comprehensive view of all types of vulnerability data. Tenable provides plugins for these products, which are scripts that complete a series of individual tests on target systems.

# Nessus

Nessus is the market leading vulnerability management solution. Nessus is available via multiple packaging options (Professional, Manager, and Cloud). Capabilities in all versions of Nessus include:

- Vulnerability assessment and basic reporting
- Broad coverage of networks, devices, systems, virtual, and cloud services
- The most comprehensive vulnerability library on the market
- Malware detection

With Nessus Cloud and Manager, you also get:

- The ability to share scan resources
- Mobile, patch and credential management system integration
- An agent-based scanning option to increase scan flexibility

## Nessus Plugin Families

Nessus plugin families are designed to allow an efficient and accurate grouping of similar security checks. This allows a user to quickly enable or disable a large group of plugins that are relevant to the target being scanned or unnecessary for a given host.

The following table summarizes the Nessus plugin families:

| Plugin Family | Description |
|---|---|
| **AIX Local Security Checks** | Security checks that test IBM AIX systems locally if authentication credentials are provided to Nessus. |
| **Amazon Linux Local Security Checks** | Security checks that test Amazon Linux systems locally if authentication credentials are provided to Nessus. |
| **Backdoors** | Plugins that detect high-profile backdoors, Trojan Horse programs, Worm infections, and systems with signs they have been compromised. |

| | |
|---|---|
| **Brute Force Attacks** | A set of plugins used to guess valid logon credentials via brute force attacks. These plugins leverage the Hydra brute force tool to perform the attacks. |
| **CentOS Local Security Checks** | Security checks that test CentOS Linux systems locally if authentication credentials are provided to Nessus. |
| **CGI abuses** | Checks for web-based CGI programs with publicly documented vulnerabilities. These checks include SQL injection, Local File Inclusion (LFI), Remote File Inclusion (RFI), Directory Traversal, and more. This family does **not** include checks for cross-site scripting (XSS). |
| **CGI abuses : XSS** | Checks for web-based CGI programs with publicly documented cross-site scripting (XSS) vulnerabilities. |
| **CISCO** | Plugins that detect vulnerabilities in Cisco routers. This family consists of both local and remote checks. Local checks will only be executed if credentials are provided to Nessus. |
| **Databases** | Checks that look for the presence of vulnerabilities in database software such as IBM DB2, Microsoft SQL Server, MySQL, Oracle Database, PostgreSQL, and more. |
| **Debian Local Security Checks** | Security checks that test Debian Linux systems locally if authentication credentials are provided to Nessus. |
| **Default Unix Accounts** | Plugins that look for the presence of default accounts found on a wide variety of Unix and Linux systems. |
| **Denial of Service** | Checks that determine the presence of Denial of Service issues by using safe methods to identify the software, not exploit the vulnerability.<br>Please refer to the Nessus User Guide for additional information about specifics when using this plugin family. |
| **DNS** | Plugins that test DNS servers such as ISC BIND and PowerDNS for known vulnerabilities. This family includes several tests that look for common issues in all DNS servers, regardless of vendor. |
| **F5 Networks Local Security Checks** | Security checks that test F5 Networks devices locally if authentication credentials are provided to Nessus. |
| **Fedora Local Security Checks** | Security checks that test Fedora Linux systems locally if authentication credentials are provided to Nessus. |
| **Firewalls** | Plugins that detect the presence of firewall devices and vulnerabilities in various commercial firewall devices, free firewall software, and proxy software. |
| **FreeBSD Local Security Checks** | Security checks that test FreeBSD systems locally if authentication credentials are provided to Nessus. |
| **FTP** | Checks that look for vulnerabilities in FTP servers. These include common issues and misconfigurations regardless of vendor, as well as vendor specific issues that have been publicly disclosed. |

| | |
|---|---|
| **Gain a shell remotely** | Plugins that test for a wide variety of software for vulnerabilities that allow for remote code or command execution. |
| **General** | A set of checks that gather information about the remote system such as operating system and service identification, network connectivity, and more. |
| **Gentoo Local Security Checks** | Security checks that test Gentoo Linux systems locally if authentication credentials are provided to Nessus. |
| **HP-UX Local Security Checks** | Security checks that test HP-UX systems locally if authentication credentials are provided to Nessus. |
| **Huawei Local Security Checks** | Security checks that test Huawei devices locally if authentication credentials are provided to Nessus. |
| **Incident Response** | A set of plugins to detect traffic anomalies used by network security professionals to hunt threats and respond to incidents. |
| **Junos Local Security Checks** | Security checks that test Juniper Junos systems locally if authentication credentials are provided to Nessus. |
| **MacOS X Local Security Checks** | Security checks that test Apple Mac OS X systems locally if authentication credentials are provided to Nessus. |
| **Mandriva Local Security Checks** | Security checks that test Mandriva Linux systems locally if authentication credentials are provided to Nessus. |
| **Misc.** | Plugins that test for a wide variety of software including client-side and server issues. |
| **Mobile Devices** | Plugins related to mobile devices such as Android-based phones and Apple portable devices such as the iPhone or iPad. |
| **Netware** | Security checks that test Novell Netware systems for vulnerabilities. |
| **Oracle Linux Local Security Checks** | Security checks that test Oracle Linux systems locally if authentication credentials are provided to Nessus. |
| **OracleVM Local Security Checks** | Security checks that test Oracle VM systems locally if authentication credentials are provided to Nessus. |
| **Palo Alto Local Security Checks** | Security checks that test Palo Alto systems and devices locally if authentication credentials are provided to Nessus. |
| **Peer-To-Peer File Sharing** | Checks that look for the presence of peer-to-peer file sharing software and associated vulnerabilities. |
| **Policy Compliance** | Plugins that are designed to verify a system meets criteria as set forth by a compliance initiative such as PCI DSS, SCAP, CIS benchmarks, and more.<br>! These plugins are only available to Nessus Professional, Nessus Manager, and Nessus Cloud customers and can be obtained from the Tenable Support Portal. |

| | |
|---|---|
| **Port Scanners** | This family contains the port scanning functionality of Nessus. |
| **Red Hat Local Security Checks** | Security checks that test Red Hat Linux systems locally if authentication credentials are provided to Nessus. |
| **RPC** | Plugins that look for the presence of vulnerabilities in Remote Procedure Call (RPC) services, NIS, NFS, and more. |
| **SCADA** | Checks that test for vulnerabilities in SCADA (supervisory control and data acquisition) software.<br>❗ These plugins are only available to Nessus Professional, Nessus Manager, and Nessus Cloud customers and can be obtained from the Tenable Support Portal. |
| **Scientific Linux Local Security Checks** | Security checks that test Scientific Linux systems locally if authentication credentials are provided to Nessus. |
| **Service detection** | Security checks that allow Nessus to detect a wide variety of services on a remote host. |
| **Settings** | Plugins that control the behavior of Nessus during a scan. |
| **Slackware Local Security Checks** | Security checks that test Slackware Linux systems locally if authentication credentials are provided to Nessus. |
| **SMTP problems** | Checks related to the Simple Mail Transfer Protocol (SMTP) and mail servers. |
| **SNMP** | Checks related to the Simple Network Management Protocol (SNMP) for a wide variety of vendors and common configuration errors. |
| **Solaris Local Security Checks** | Security checks that test Oracle Solaris systems locally if authentication credentials are provided to Nessus. |
| **SuSE Local Security Checks** | Security checks that test SUSE Linux systems locally if authentication credentials are provided to Nessus. |
| **Ubuntu Local Security Checks** | Security checks that test Ubuntu Linux systems locally if authentication credentials are provided to Nessus. |
| **VMware ESX Local Security Checks** | Security checks that test VMware ESX systems locally if authentication credentials are provided to Nessus. |
| **Web Servers** | Plugins that check for vulnerabilities in web servers such as Apache HTTP Server, IBM Lotus Domino, Microsoft IIS, and many more. Note: These checks only test the web server software, not the web applications hosted on the server. |
| **Windows** | Checks for software installed on Microsoft Windows systems including Adobe Reader, Adobe Flash, Antivirus software, web browsers, iTunes, and much more. |
| **Windows : Microsoft Bulletins** | Security checks that test Microsoft Windows systems locally if authentication credentials are provided to Nessus. |

| | |
|---|---|
| **Windows : User management** | Plugins that check for issues in Microsoft Windows user management. These include user information disclosure, group enumeration, and more. |

Historically, Nessus has used additional families for plugin organization that were deprecated at some point. Their plugins have been integrated into current families.

## Passive Vulnerability Scanner

Tenable Passive Vulnerability Scanner (U.S. patent 7,761,918 B2) is a network discovery and vulnerability analysis software solution that delivers continuous network listening, profiling, and monitoring in a non-intrusive manner.

The Passive Vulnerability Scanner monitors network traffic at the packet layer to determine topology, services, and vulnerabilities and is tightly integrated with Tenable's SecurityCenter and Log Correlation Engine to centralize both event analysis and vulnerability management for a complete view of your security and compliance posture.

### PVS Plugin Families

The PVS has two sources of "plugin" information: the **.prmx** and **.prm** plugin libraries in the **plugins** directory and the operating system fingerprints in the **osfingerprints.txt** file.

Tenable distributes its passive vulnerability plugin database in an encrypted format. This file is known as **tenable_plugins.prmx** and can be updated on a daily basis, if necessary. PVS plugins that are written by the customer or third parties have the extension of **.prm**.

The following table summarizes the Tenable PVS plugin families:

| Plugin Family | Description |
|---|---|
| **Backdoors** | Plugins that detect a variety of indications that a system or application has been compromised, and potentially backdoored for persistent access. |
| **CGI** | A variety of plugins that check for the presence of CGI programs, web applications, and vulnerabilities associated with them. |
| **Cloud Services** | Plugins that detect the use of cloud services such as Salesforce, Dropbox, and Amazon Cloud. |
| **Database** | Passive detection of database software and associated vulnerabilities. |
| **Data Leakage** | Plugins that look for signs of confidential information traversing the network (e.g., Social Security numbers). |
| **DNS Servers** | Checks related to DNS servers and suspicious DNS traffic. |
| **Finger** | Detection and vulnerabilities related to the Finger protocol. |

| | |
|---|---|
| **FTP Clients** | Plugins that detect FTP client software and vulnerabilities associated with it. |
| **FTP Servers** | Plugins that detect FTP servers and vulnerabilities associated with it. |
| **Generic** | This family contains plugins that do not fit in the other families. |
| **IMAP Servers** | Detection of Internet Message Access Protocol (IMAP) servers and associated vulnerabilities. |
| **Internet Messengers** | Plugins that monitor for Instant Messenger software such as AIM, Yahoo Messenger, and ICQ. |
| **Internet Services** | Checks that detect traffic to Internet services such as Facebook, Twitter, Netflix, XM radio, or offsite file storage. |
| **IoT** | A set of plugins to detect traffic and vulnerabilities in Internet of Things (IoT) devices. IoT devices include thermostats, cameras, and other devices connected to a network for data collection and management. |
| **IRC Clients** | A set of plugins to detect traffic and vulnerabilities in IRC client software. |
| **IRC Servers** | A set of plugins to detect traffic and vulnerabilities in IRC servers. |
| **Malware** | Plugins that detect the presence of malware as it traverses a network. |
| **Mobile Devices** | Checks that look for any traffic or vulnerabilities related to mobile devices such as smart phones and tablets. |
| **Operating System Detection** | Plugins that monitor traffic to detect the operating system of hosts on the network. |
| **Peer-To-Peer File Sharing** | Checks that look for Peer-to-Peer traffic indicating file sharing activity. |
| **Policy** | Detects traffic that may violate corporate policy such as pornography, questionable software, or the user of third-party services that may be of concern. |
| **POP Server** | Detection of Post Office Protocol (POP) servers and associated vulnerabilities. |
| **RPC** | Plugins that detect Remote Procedure Call traffic and associated vulnerabilities. |
| **Samba** | Checks that look for Samba traffic, for file and print sharing. |
| **SCADA** | Plugins that monitor for Supervisory Control And Data Acquisition (SCADA) devices, protocols, and vulnerabilities. |
| **SMTP Clients** | A set of plugins to detect traffic and vulnerabilities in Simple Mail Transfer Protocol (SMTP) client software. |
| **SMTP Servers** | A set of plugins to detect traffic and vulnerabilities in Simple Mail Transfer Protocol (SMTP) servers. |

| | |
|---|---|
| **SNMP** | Checks related to the Simple Network Management Protocol (SNMP) for a wide variety of vendors and common configuration errors. |
| **SSH** | Plugins that detect Secure Shell (SSH) traffic. |
| **Web Clients** | A set of plugins to detect traffic and vulnerabilities in HTTP and HTTPS clients such as web browsers. |
| **Web Servers** | A set of plugins to detect traffic and vulnerabilities in web servers. |

Historically, PVS has used additional families for plugin organization that were deprecated at some point. Their plugins have been integrated into current families.

## Log Correlation Engine

Tenable Network Security's Log Correlation Engine (LCE) product offers many types of event correlation to detect abuse, anomalies compromise, and compliance violations. The LCE normalizes events into a variety of types. For reference, each type and a description for it are listed here.

### LCE Event Types and Plugin Families

The LCE plugins are located in the **`/opt/lce/daemons/plugins`** directory. To optimize plugin performance, it is suggested that the **`plugin_manager.sh`** script be used. The **`plugin_manager.sh`** script is located in the **`/opt/lce/tools`** directory. When run, it will report on the number of installed plugin libraries that have never been used, and prompt you to disable the associated files. You may choose not to do so if you wish to review a full report prior to making any changes. In this case, the script will list the unused files.

The following table summarizes the LCE event types:

| Event Types | Description |
|---|---|
| **access-denied** | Flags attempts to retrieve objects, files, network shares, and other resources that are denied. These events are distinct from authentication failures, blocked firewall connections, and attempts to access web pages that do not exist that are respectively normalized to the login-failure, firewall, and web-error event types. |
| **application** | Denotes logs from any application such as Nessus, Symantec Anti-Virus, SecurityCenter, the WU-FTP server, Sendmail, etc. that is noteworthy but not indicative of an error, a login failure, a connection, a restart of the application, an operating system event, or a major function of the device. |
| **connection** | Notes any type of audited network connection that is not directly logged via the Tenable NetFlow Monitor (TFM) or the Tenable Network Monitor (TNM). Event sources include allowed connections through firewalls, established VPN sessions, and connections by some types of applications. |

| | |
|---|---|
| **continuous** | The LCE can identify hosts that are generating specific event types for periods of 20 minutes or longer. |
| **data-leak** | Flags logs from the PVS or other Data Leak Prevention products that indicate the presence of sensitive data such as a credit card or Social Security number. |
| **database** | Denotes logs generated by the PVS from observed SQL queries. |
| **detected-change** | The LCE automatically recognizes many types of system events that indicate change and creates secondary higher level events. |
| **dhcp** | Logs from DHCP servers that indicate new leases are given the DHCP event type. |
| **dns** | Denotes any type of log from a DNS server or from real-time network monitoring by the PVS that indicates a DNS query or a DNS query lookup failure. LCE summary information as well as Fast Flux detection is also logged here. |
| **dos** | Denotes logs that indicate a denial of service event has occurred. These typically occur from network IDS detection engines such as Snort. |
| **error** | Denotes any type of system, application, router, or switch log that indicates some sort of error. Logs that indicate crashes and hung process are sent to the process event type. |
| **file-access** | Denotes any type of sniffed PVS network session or log that indicates that a file was accessed, modified, or likely retrieved. |
| **firewall** | Denotes any type of log from a firewall, an intrusion prevention device, a router, or a firewall or application configured at the local host to specifically deny connections. |
| **honeypot** | Indicates logs that are normalized from applications designed to simulate networks, hosts, and applications for the purpose of detecting intruders. |
| **Indicator** | The "indicator" event type is used by LCE to track correlations associated with scanning, compromises, anomalies, and other behaviors that indicate the presence of determined attackers, advanced malware, and other forms of potentially malicious activities. |
| **intrusion** | Denotes logs from network IDS, firewall, application, and operating systems that indicate some sort of network attack. Post scans, denial of service, and logs that indicate virus probes are normalized to their own LCE event types. |
| **lce** | The LCE includes this distinct event type to assist in tracking information about LCE clients such as the LCE Windows client, LCE Linux client, LCE NetFlow Monitor (TFM), and the LCE Network Monitor (TNM). |
| **login** | Indicates any type of login event to an application, operating system, VPN, firewall, or other type of device. |
| **login-failure** | Denotes any type of authentication log that indicates credentials were presented and were incorrect. |
| **logout** | The LCE normalizes events for applications, operating systems, and devices that detect when a user's session is finished to the logout event type. |

| | |
|---|---|
| **nbs** | The LCE tracks all normalized events that have occurred for each host. As new normalized events are logged for the host, the LCE will generate secondary events based on the event type. |
| **network** | Logs from the Tenable NetFlow Monitor (TFM) and the Tenable Network Monitor (TNM) are logged to this LCE event type. |
| **process** | Logs from Unix process accounting and Windows event logs that indicate process starts and stops, as well as executable crashes, restarts, hung states, and segmentation faults are logged to this LCE event type. |
| **restart** | The LCE will normalize logs from when applications, services, router, switches, devices, and operating systems reboot, restart, and are shutdown to the restart event type. |
| **social-networks** | The PVS detects a wide variety of social network activity such as Bing searches, logins to Gmail, Facebook, Wikipedia searches, Twitter, and generic passively discovered IMAP and POP access. These are logged to the social-networks LCE event type. Some event examples are shown below. |
| **scanning** | Network IDS, firewall, antivirus, and other log sources that detect port scans, port sweeps, and probes are logged to the LCE scanning event type. |
| **spam** | Logs from email servers, antivirus email tools, SPAM appliances, firewalls, and other sources that indicate spam activity are normalized to the LCE spam event type. |
| **stats** | For every unique type of event, the LCE will profile the frequency of events and alert when there is a statistical deviation for any event. |
| **system** | The LCE will normalize operating system, router, switch, or device logs of significance to the event type of system. Login failures, errors, and application events are logged to other event types. |
| **threatlist** | The LCE maintains a list of hostile IPv4 addresses and domains that are known to be participating in botnets. |
| **usb** | The LCE windows client can detect USB and CD-ROM insertions and removals. The logs generated by these events are normalized to the USB event type. |
| **virus** | Logs that indicate the presence of a virus in email, a virus found on a system by an anti-virus agent, virus logs found by network IDS events and firewalls are normalized to the LCE event type of virus. |
| **vulnerability** | As security issues and new information about systems and networks are reported as part of the vulnerability monitoring process, the LCE normalizes these event types to the vulnerability category. |
| **web-access** | Any type of log that indicates a successful connection to a web resource is normalized as a web-access LCE event type. |
| **web-error** | Denotes any type of web access event that is denied because the file does not exist, the server responded with an error or a firewall or web application firewall blocked the access. |

The Event Vulnerability plugin families below work along with the other Tenable plugin families. These plugin families use Nessus scan results, PVS results, and LCE host analysis to correlate data together that can then be viewed in SecurityCenter CV.

| Plugin Family | Description |
|---|---|
| Database | Passive detection of database software and associated vulnerabilities. |
| DNS Servers | Denotes any type of log from a DNS server or from real-time network monitoring by PVS that indicates a DNS query or a DNS query lookup failure. LCE summary information as well as Fast Flux detection is also logged here. |
| FTP Servers | Plugins that detect FTP servers and vulnerabilities associated with it. |
| Generic | This family contains plugins that do not fit in the other families. |
| IMAP Servers | Detection of Internet Message Access Protocol (IMAP) servers and associated vulnerabilities. |
| IRC Clients | A set of plugins to detect traffic and vulnerabilities in IRC client software. |
| Mobile Devices | Checks that look for any traffic or vulnerabilities related to mobile devices such as smart phones and tablets. |
| Operating System Detection | Plugins that monitor traffic to detect the operating system of hosts on the network. |
| Policy | Detects traffic that may violate corporate policy such as pornography, questionable software, or the use of third-party services that may be of concern. |
| RPC | Plugins that detect Remote Procedure Call traffic and associated vulnerabilities. |
| Samba | Checks that look for Samba traffic, for file and print sharing. |
| SMTP Clients | A set of plugins to detect traffic and vulnerabilities in Simple Mail Transfer Protocol (SMTP) client software |
| SMTP Servers | A set of plugins to detect traffic and vulnerabilities in Simple Mail Transfer Protocol (SMTP) servers. |
| SNMP | Checks related to the Simple Network Management Protocol (SNMP) for a wide variety of vendors and common configuration errors. |
| SSH | Plugins that detect Secure Shell (SSH) traffic. |
| Web Clients | A set of plugins to detect traffic and vulnerabilities in HTTP and HTTPS clients such as web browsers. |
| Web Servers | A set of plugins to detect traffic and vulnerabilities in web servers. |

Historically, LCE has used additional families for plugin organization that were deprecated at some point. Their plugins have been integrated into current families.

## For More Information

For more information on Tenable plugins and documentation, please refer to the following:

Product User Guides:
https://docs.tenable.com/

Full list of Nessus plugins:
http://www.tenable.com/plugins/index.php?view=all

Nessus Discussions Forum:
https://discussions.tenable.com/

PVS RSS Feed:
http://www.tenable.com/pvs.xml

PVS Plugins:
http://static.tenable.com/dev/tenable_plugins.pdf

LCE Best Practices:
http://www.tenable.com/whitepapers/log-correlation-engine-best-practices

Tenable Event Correlation:
https://www.tenable.com/whitepapers/tenable-event-correlation

## About Tenable Network Security

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail, and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.