



## Network Security Package for TN-4900 Series Release Notes

<b>Version: v10.0.31</b>	<b>Build: 25052914</b>
<b>Release Date: Jun 20, 2025</b>	

### Applicable Products

TN-4900 Series

### Supported Operating Systems

N/A

### New Features

- Added support for IPS pattern v1.134.
- [Web Squid Proxy] ESI Response Processing nullpointer Denial of Service (CVE-2024-45802) (Pattern ID: 1232787, 1232788, 1232833)
- [Zimbra Collaboration] Proxy Servlet Server Side Request Forgery (CVE-2024-45518) (Pattern ID: 1232798)
- [SonicWall SonicOS SSLVPN] getSslvpnSessionFromCookie Authentication Bypass (CVE-2024-53704) (Pattern ID: 1232830, 1232835, 1232836, 1232837)
- [Nagios XI] historytab\_content.php SQL Injection (Pattern ID: 1232838, 1232839)
- [Adobe ColdFusion] invokeLoggingModule Directory Traversal (CVE-2024-53961) (Pattern ID: 1232841)
- [Ivanti Endpoint Manager] DPIDatabase GetComputerID SQL Injection (CVE-2024-50330) (Pattern ID: 1232843)
- [Apache OpenMeetings] Cluster Mode Insecure Deserialization (CVE-2024-54676) (Pattern ID: 1232844)
- [Wazuh] as\_wazuh\_object Insecure Deserialization (CVE-2025-24016) (Pattern ID: 1232845, 1232846)
- [VMware HCX] listExtensions SQL Injection (CVE-2024-38814) (Pattern ID: 1232848)
- [OpenSSL] do\_x509\_check Name Check Denial of Service (CVE-2024-6119) (Pattern ID: 1232849)
- [Apache Tomcat] Partial PUT Path Equivalence (CVE-2025-24813) (Pattern ID: 1232850)
- [LibreNMS] Device Misc dynamic\_override\_config Stored Cross-Site Scripting (CVE-2025-23200) (Pattern ID: 1232852)
- [Sitecore] Multiple Products ThumbnailsAccessToken Insecure Deserialization (CVE-2025-27218) (Pattern ID: 1232853)
- [HPE Insight Remote Support] processAttachmentDataStream Directory Traversal (CVE-2024-53676) (Pattern ID: 1232854)
- [Ivanti Endpoint Manager] ECustomDataForm OnSaveToDB Directory Traversal (CVE-2024-50322, CVE-2024-50330) (Pattern ID: 1232855, 1232857)
- [HPE Insight Remote Support] setInputStream XML External Entity Injection (CVE-2024-11622) (Pattern ID: 1232858, 1232859)
- [Apache Tomcat] JSP Compilation Race Condition (CVE-2024-50379) (Pattern ID: 1232860)
- [Next.js] Middleware Bypass Vulnerability (CVE-2025-29927) (Pattern ID: 1232861)
- [Cacti] host\_templates.php template SQL Injection (CVE-2024-54146) (Pattern ID: 1232866)
- [Gogs] Repository Contents API Path Traversal (CVE-2024-55947), GetDiffPreview Argument Injection (CVE-2024-39932) (Pattern ID: 1232867, 1232895)
- [Apache Camel] DefaultHeaderFilterStrategy Improper Filtering (CVE-2025-27636) (Pattern ID: 1232813, 1232863, 1232864)
- [LibreNMS] Device Port Settings Description Stored Cross-Site Scripting (CVE-2025-23199) (Pattern ID: 1232872)
- [Progress Kemp LoadMaster] mangle Stack-based Buffer Overflow (CVE-2025-1758) (Pattern ID:



1232873)

- [FortiGuard Labs FortiOS and FortiProxy] Node.js websocket Authentication Bypass (CVE-2024-55591) (Pattern ID: 1232874)
- [Progress WhatsUp Gold] GetSqlWhereClause SQL Injection (CVE-2024-46906) (Pattern ID: 1232875)
- [Microsoft Windows] searchConnectorms and library-ms Files NTLM Relay (CVE-2025-24054) (Pattern ID: 1232876)
- [Linux Kernel ksmbd] TCP Connection Memory Exhaustion Denial-of-Service (CVE-2024-50285) (Pattern ID: 1232868)
- [Ivanti Cloud Services Application] SendAlert Command Injection (CVE-2024-47908) (Pattern ID: 1232877, 1232878)
- [Rsync Daemon] Checksum Handling Heap-based Buffer Overflow (CVE-2024-12084) (Pattern ID: 1232879)
- [Commvault] Pre-Authenticated Remote Code Execution (CVE-2025-34028) (Pattern ID: 1232880)
- [Django] wordwrap Filter Denial of Service (CVE-2025-26699) (Pattern ID: 1232881)
- [Ivanti Endpoint Manager] MP\_QueryDetail SQL Injection (CVE-2024-34781) (Pattern ID: 1232883)
- [CyberPanel] filemanager.py upload Command Injection (CVE-2024-51568), getresetstatus Command Injection (CVE-2024-51378) (Pattern ID: 1232886, 1232772, 1232775)
- [Pandora FMS] chromium\_path and phantomjs\_bin Command Injection (CVE-2024-12971) (Pattern ID: 1232887)
- [AI] POE access via SSL (Pattern ID: 1165264), Perplexity access via SSL (Pattern ID: 1165265), Claude access via SSL (Pattern ID: 1165266)
- [OpenEMR] Bronchitis Form Stored Cross-Site Scripting (CVE-2025-30161) (Pattern ID: 1232892, 1232893)
- [FlowiseAI] Flowise attachments Directory Traversal (CVE-2025-26319) (Pattern ID: 1232894)
- [Fortinet FortiSandbox] VM Download Command Injection (CVE-2024-52961) (Pattern ID: 1232896)
- [Microsoft Scripting Engine] Memory Corruption Vulnerability (CVE-2017-8605) (Pattern ID: 1133829)

## **Enhancements**

N/A

## **Bugs Fixed**

N/A

## **Changes**

N/A

## **Notes**

- The following outdated or deprecated IPS patterns have been removed to improve system efficiency and focus on relevant threats:
  - Legacy vulnerabilities in Microsoft Windows Shell, SAP GUI, Adobe Flash, and others from 2017 (Pattern ID: 1134116, 1134122, 1134123, 1134125, 1134129, 1134131, 1134134, 1134135, 1134136, 1134138, 1134140, 1134142, 1134143, 1134148, 1134151, 1134153, 1134154, 1134156, 1134160,



1134161, 1134163, 1134164, 1134166, 1134167, 1134168, 1134172, 1134174)

- Deprecated issues in Microsoft Edge, HPE Intelligent Management Center, Adobe Flash Player (Pattern ID: 1134027, 1134051, 1134052, 1134060, 1134061, 1134062, 1134063)
- Outdated patterns related to Internet Explorer, PostgreSQL, and Mozilla Firefox (Pattern ID: 1133974, 1133975, 1133985, 1134014, 1134015, 1134016)
- DNS and image-processing vulnerabilities in BIND, systemd, and PHP libraries (Pattern ID: 1133901, 1133919, 1133945, 1133952)
- Old exploits in Microsoft Edge, Samba, and IPFire (Pattern ID: 1133829, 1133830, 1133831, 1133854, 1133886)
- Deprecated Apache Struts2 Remote Code Execution vulnerability (Pattern ID: 1232751)
- Historical vulnerabilities in PHP and Microsoft browsers (Pattern ID: 1133297, 1134084)

<b>Version: v10.0.28</b>	<b>Build: 25022514</b>
<b>Release Date: Mar 31, 2025</b>	

## Applicable Products

TN-4900 Series

## Supported Operating Systems

N/A

## New Features

- Added support for IPS pattern v1.1.121.
- [QNAP HBS 3 Hybrid Backup Sync] Added protection against command injection targeting NAS devices. (CVE-2024-50388) (Pattern ID: 1232774, 1232776)
- [Ivanti Cloud Services Appliance] Added SQL injection protection for cloud appliance configuration APIs. (CVE-2024-11773) (Pattern ID: 1232780, 1232781)
- [Ivanti Endpoint Manager] Directory traversal and SQL injection protection for endpoint configuration. (CVE-2024-34787, CVE-2024-50326) (Pattern ID: 1232783, 1232790)
- [Rockwell ThinManager] Directory traversal protection for ThinServer.exe API interface. (CVE-2024-45826) (Pattern ID: 1232784)
- [Jenkins] Arbitrary file read defense in Remoting module. (CVE-2024-43044) (Pattern ID: 1232678)
- [Grafana] Command injection and local file inclusion protections. (CVE-2024-9264) (Pattern ID: 1232732)
- [LibreNMS] Multiple protections, including command injection and stored XSS for device settings. (CVE-2024-51092, CVE-2024-53457, CVE-2024-49754) (Pattern ID: 1232730, 1232789, 1232796)
- [Nagios XI] Command injection protection in windows-winrm component. (Pattern ID: 1232800)
- [Palo Alto PAN-OS] Authentication bypass and command injection fixes. (CVE-2024-0012, CVE-2024-9474) (Pattern ID: 1232734, 1232735)
- [JetBrains TeamCity] Stored cross-site scripting vulnerabilities resolved. (CVE-2024-47951) (Pattern ID: 1232736, 1232737, 1232738, 1232739)
- [Delta InfraSuite] Insecure deserialization protection. (CVE-2024-10456) (Pattern ID: 1232740)
- [Apache Traffic Control] SQL injection prevention in delivery service comments. (CVE-2024-45387) (Pattern ID: 1232794)
- [Microsoft Configuration Manager] SQL injection protection added. (CVE-2024-43468) (Pattern ID: 1232795)
- [WordPress Tutor LMS Plugin] SQL injection vulnerabilities patched. (CVE-2024-10400) (Pattern ID: 1232801, 1232802)
- [WordPress WP Time Capsule Plugin] File upload restriction enforced. (CVE-2024-8856) (Pattern ID: 1232803)
- [Palo Alto Networks Expedition] Deserialization attack defense. (CVE-2025-0107) (Pattern ID: 1232804)
- [Apache Solr] Directory traversal vulnerability addressed. (CVE-2024-52012) (Pattern ID: 1232805)



- [Microsoft Windows LDAP] Memory and buffer vulnerabilities protected. (CVE-2024-49112, CVE-2024-49113) (Pattern ID: 1232806, 1232807)

### **Enhancements**

N/A

### **Bugs Fixed**

N/A

### **Changes**

N/A

### **Notes**

- The following outdated or deprecated IPS patterns have been removed to improve system efficiency and focus on relevant threats:
  - WEB Flexense VX Search Enterprise add\_command Buffer Overflow (Pattern ID: 1134308, 1134309)
  - WEB Oracle Identity Manager Default Credentials (Pattern ID: 1134312, 1134313)
  - GitLab Gollum Link Regex DoS (Pattern ID: 1232596)
  - QNAP Log Upload Command Injection (Pattern ID: 1232603)
  - Old vulnerabilities in Adobe, Chrome, Windows SMB, Exim, HPE, etc. from 2017 (Pattern ID: 1134253, 1134254, 1134255, 1134257, 1134258, 1134264, 1134265, 1134269, 1134270, 1134274, 1134275, 1134276, 1134277, 1134299, 1134305, 1232623)
  - Legacy Microsoft and Apache Solr vulnerabilities (Pattern ID: 1134214, 1134217, 1134219, 1134220, 1134225, 1134231, 1134232, 1134238)



<b>Version: v10.0.26</b>	<b>Build: 24122710</b>
<b>Release Date: Jan 20, 2025</b>	

### **Applicable Products**

TN-4900 Series

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

- Added support for IPS pattern v1.111.

### **Bugs Fixed**

N/A

### **Changes**

N/A

### **Notes**

N/A



<b>Version: v10.0.25</b>	<b>Build: 24120610</b>
<b>Release Date: Dec 20, 2024</b>	

### **Applicable Products**

TN-4900 Series

### **Supported Operating Systems**

N/A

### **New Features**

- Added support for IPS pattern v1.107.

### **Enhancements**

- DPI policy rules show an incorrect interface name if VRRP is enabled.

### **Bugs Fixed**

N/A

### **Changes**

N/A

### **Notes**

N/A



<b>Version: v10.0.23</b>	<b>Build: 24102510</b>
<b>Release Date: Nov 12, 2024</b>	

### **Applicable Products**

TN-4900 Series

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

- Added support for IPS pattern v1.102.

### **Bugs Fixed**

N/A

### **Changes**

- Aligned the MXsecurity Agent Package version format in the interface.

### **Notes**

N/A



<b>Version: v10.0.20</b>	<b>Build: 24092013</b>
<b>Release Date: Oct 09, 2024</b>	

### **Applicable Products**

TN-4900 Series

### **Supported Operating Systems**

N/A

### **New Features**

- Added support for new DPI protocols to Advanced Protection: Step7 Comm+, OPC UA, MELSEC.
- Added support for IPS pattern v1.094.

### **Enhancements**

N/A

### **Bugs Fixed**

N/A

### **Changes**

N/A

### **Notes**

N/A





<b>Version: v9.0.12</b>	<b>Build: 24080111</b>
<b>Release Date: Aug 30, 2024</b>	

### **Applicable Products**

TN-4900 Series

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

- Added support for IPS pattern v1.0.89.
- Added an IPS pattern to protect against CVE-2024-6387 (OpenSSH vulnerability issue).

### **Bugs Fixed**

- The IEC-104 protocol filter will unexpectedly block STARTDT packets.

### **Changes**

N/A

### **Notes**

N/A



<b>Version: v8.0.20</b>	<b>Build: 24062714</b>
<b>Release Date: Jul 12, 2024</b>	

### **Applicable Products**

TN-4900 Series

### **Supported Operating Systems**

N/A

### **New Features**

- Updated the IPS pattern version to v1.085.

### **Enhancements**

N/A

### **Bugs Fixed**

N/A

### **Changes**

N/A

### **Notes**

N/A



<b>Version: v8.0.17</b>	<b>Build: 24043014</b>
<b>Release Date: May 07, 2024</b>	

### **Applicable Products**

TN-4900 Series

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

- Updated the IPS pattern version to v1.076.

### **Bugs Fixed**

N/A

### **Changes**

N/A

### **Notes**

N/A



<b>Version:</b> v8.0.15	<b>Build:</b> 24032616
<b>Release Date:</b> May 06, 2024	

### **Applicable Products**

TN-4900 Series

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

- Updated the IPS pattern version to v1.072.

### **Bugs Fixed**

N/A

### **Changes**

N/A

### **Notes**

N/A



<b>Version: v8.0.13</b>	<b>Build: 24013111</b>
<b>Release Date: Jan 31, 2024</b>	

### **Applicable Products**

TN-4900 Series

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

- Updated the IPS pattern version to v1.064.□

### **Bugs Fixed**

N/A

### **Changes**

N/A

### **Notes**

N/A



<b>Version: v8.0.12</b>	<b>Build: 23122612</b>
<b>Release Date: Dec 26, 2023</b>	

### **Applicable Products**

TN-4900 Series

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

- Updated the IPS pattern version to v1.059.

### **Bugs Fixed**

N/A

### **Changes**

N/A

### **Notes**

- Security Package v7.0.16 function is integrated into v8.0.12.



<b>Version: v7.0.16</b>	<b>Build: 23112911</b>
<b>Release Date: Nov 29, 2023</b>	

### **Applicable Products**

TN-4900 Series

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

- Updated the IPS pattern version to v1.055.□

### **Bugs Fixed**

N/A

### **Changes**

N/A

### **Notes**

N/A



<b>Version: v7.0.12</b>	<b>Build: 23081018</b>
<b>Release Date: Aug 10, 2023</b>	

### **Applicable Products**

TN-4900 Series

### **Supported Operating Systems**

N/A

### **New Features**

- Added support for IPS functionality.
- Added support for Industrial Protocol DPI: TRDP.

### **Enhancements**

- Updated the IPS pattern version to v1.039.

### **Bugs Fixed**

N/A

### **Changes**

N/A

### **Notes**

N/A