Network Security Package for EDR-G9010 Series Release Notes

Version: v10.0.31	Build: 25052914
Release Date: Jun 20, 2025	

Applicable Products

EDR-G9010 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] processAtatchmentDataStream 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)

Version: v10.0.28	**Build: 25022514**
Release Date: Mar 31, 2025	

Applicable Products

EDR-G9010 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)

Version: v10.0.26	Build: 24122710
Release Date: Jan 20, 2025	

Applicable Products

EDR-G9010 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

Version: v10.0.25	Build: 24120610
Release Date: Dec 20, 2024	

Applicable Products

EDR-G9010 Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Added support for IPS pattern v1.107.

Bugs Fixed

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

Changes

N/A

Notes

N/A

Version: v10.0.23	Build: 24102510
Release Date: Nov 12, 2024	

Applicable Products

EDR-G9010 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

Version: v10.0.20	Build: 24092013
Release Date: Oct 09, 2024	

Applicable Products

EDR-G9010 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

Version: v9.0.12	Build: 24080111
Release Date: Aug 30, 2024	

Applicable Products

N/A

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

Version: v8.0.20	Build: 24062714
Release Date: Jul 12, 2024	

Applicable Products

N/A

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

Version: v8.0.17	Build: 24043014
Release Date: May 07, 2024	

Applicable Products

N/A

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

Version: v8.0.12	Build: 23122611
Release Date: Dec 26, 2023	

Applicable Products

N/A

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

N/A

Version: v6.0.21	Build: 23112910
Release Date: Nov 29, 2023	

Applicable Products

N/A

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

Version: v6.0.17	Build: 23081017
Release Date: Aug 10, 2023	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

• Added support for Industrial DPI protocols: EIP, Omron FINS, Step 7.

Enhancements

• Updated the IPS pattern version to v1.038.

Bugs Fixed

N/A

Changes

N/A

Notes

N/A

Version: v5.0.39	Build: 23062713
Release Date: Jul 03, 2023	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Updated the IPS pattern version to v1.038.

Bugs Fixed

N/A

Changes

N/A

Notes

N/A

Version: v5.0.37	Build: 23042613
Release Date: May 02, 2023	

Applicable Products

EDR-G9010 Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Updated the IPS pattern version to v1.033.

Bugs Fixed

N/A

Changes

N/A

Notes

N/A

Version: v5.0.36	Build: 23032815
Release Date: Mar 29, 2023	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Updated the IPS pattern version to v1.029.

Bugs Fixed

N/A

Changes

N/A

Notes

N/A

Version: v5.0.35	Build: 23022217
Release Date: Mar 08, 2023	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Updated the IPS pattern version to v1.023.

Bugs Fixed

• The system shows abnormal memory use due to a memory leak.

Changes

N/A

Notes

N/A

Version: v5.0.34	Build: 23020217
Release Date: Feb 06, 2023	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Updated the IPS pattern version to v1.021.

Bugs Fixed

• The Modbus protocol filter behaves abnormally for function code 23.

Changes

N/A

Notes

This version is only compatible with firmware v2.0 or higher.

Version: v5.0.33	Build: N/A
Release Date: Jan 06, 2023	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Updated the IPS pattern version to v1.016.

Bugs Fixed

• When upgrading the network security package from v3.x to v5.0.x, the Action of all IPS rules is set to Accept.

Changes

N/A

Notes

N/A

Version: v5.0.30	Build: 22112510
Release Date: Nov 30, 2022	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Updated the IPS pattern version to v1.009.

Bugs Fixed

N/A

Changes

N/A

Notes

This version is only compatible with firmware v2.0 or higher.

Version: v5.0.29	Build: 22090817
Release Date: Sep 26, 2022	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Updated the web user interface to the latest next-generation design.

Bugs Fixed

N/A

Changes

N/A

Notes

• This version is only compatible with firmware v2.0 or higher.

Version: v3.0.24	Build: 22031518
Release Date: Mar 18, 2022	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• Modbus TCP communication behaves abnormally after installing the security package.

Changes

N/A

Notes

N/A

Version: v3.0.23	Build: 22011918
Release Date: Jan 24, 2022	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

• Added support for the IEC 104 and MMS protocols for the Application Firewall.

Enhancements

• Added a global default rule setting to Enforcement Settings.

Bugs Fixed

• The system crashes when receiving a Modbus packet with an incorrect length.
• Application firewall rules continue to exist after being deleted.
• ADP index 1000014 behaves abnormally with specific sub-functions.
• The SYN-Flood Denial of Service (DoS) setting behaves abnormally after installing a security package.

Changes

• Changed the maximum supported number of protocol filter rules from 512 to 200.

Notes

N/A

Version: v2.0.48	Build: 21120114
Release Date: Dec 02, 2021	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• The DNP3 packet filtering Layer 3 policy does not work correctly after installing the security package.
• The ADP setting is reset to its default value after upgrading the security package.

Changes

• Removed the "Stateful" option from the "Command type" selection in the Rule settings window.
• Changed the action for the Master Query and Slave Response command types from "Drop" to "Reset".
• Removed the "Bridge interface" option in the policy settings window.

Notes

Known Issue - V2.0.45
• Protocol filtering does not work properly when using "Stateful" as the command type, or when using a bridge interface. Version 2.0.48 temporarily removes these two options to avoid unexpected behavior until the issue is resolved.

Version: v2.0.45	Build: 21092711
Release Date: Oct 05, 2021	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

The first release of the EDR-G9010 Series Security Package.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A