



Network Security Package for EDR-G9004 Series Release Notes

Version: v13.0.27	Build: 25102218
Release Date: Nov 07, 2025	

Applicable Products

EDR-G9004 Series

Supported Operating Systems

N/A

New Features

- Added support for IPS pattern v1.156.
- [JetBrains TeamCity] Directory traversal vulnerability mitigated in uploadArchive (CVE-2025-59456) (Pattern ID: 1233089)
- [Microsoft Windows NetLogon Service] Denial-of-service vulnerability addressed in NetrServerReqChallenge process (CVE-2025-26673) (Pattern ID: 1233090, 1233091)
- [Fortinet FortiWeb] Directory traversal vulnerability mitigated in _cmf_get_config_file_path (CVE-2025-53609) (Pattern ID: 1233092)
- [Ivanti Endpoint Manager] Arbitrary file write vulnerabilities resolved in EFile CreateFile module (CVE-2025-9712) (Pattern ID: 1233093, 1233094)
- [Cisco Identity Services Engine] Insecure deserialization vulnerability fixed in handleStrongSwanTunnelStatus (CVE-2025-20284) (Pattern ID: 1233069)
- [WordPress Everest Forms Plugin] Unrestricted file upload vulnerability mitigated (CVE-2025-1128) (Pattern ID: 1233070)
- [LibreNMS] Stored cross-site scripting vulnerability resolved in Alert Template (CVE-2025-55296) (Pattern ID: 1233074)

Enhancements

N/A

Bugs Fixed

N/A

Changes

- The following IPS patterns have been modified or updated to improve system efficiency:
 - [Brute Force Login] Detection signature updated for improved accuracy (Pattern ID: 1134083)
 - [Eicar test string] Signature maintenance update (Pattern ID: 1051723)

Notes

- The following outdated or deprecated IPS patterns have been removed to improve system efficiency and focus on relevant threats:
 - [Ivanti Connect Secure / Policy Secure] OpenSSL CRLF Injection (CVE-2024-37404) (Pattern ID: 1232713)
 - [CyberPanel] filemanager.py Command Injection (CVE-2024-51568) (Pattern ID: 1232886)
 - [Pandora FMS] chromium_path / phantomjs_bin Command Injection (CVE-2024-12971) (Pattern ID: 1232887)
 - [JetBrains TeamCity] Backup History Stored Cross-Site Scripting (CVE-2024-47950) (Pattern ID: 1232697, 1232700)
 - [Ivanti Endpoint Manager] ETask WasPreviouslyMapped SQL Injection (CVE-2024-8191) (Pattern ID: 1232701)
 - [Ivanti Avalanche] WLAvalancheService.exe Type 101/102 NULL Pointer Dereference (CVE-2024-47007) (Pattern ID: 1232702)



- [SMB Protocol] SMB2_SIGNING_CAPABILITIES Denial of Service (CVE-2024-43642) (Pattern ID: 1232707)
- [Fortinet FortiWeb] Certificate Import Format String Vulnerability (CVE-2024-45324) (Pattern ID: 1232903)

Version: v13.0.26	Build: 25092416
Release Date: Oct 01, 2025	

Applicable Products

EDR-G9004 Series

Supported Operating Systems

N/A

New Features

- [Grafana Labs Grafana] Scripted Dashboard Reflected XSS (CVE-2025-6023) (Pattern ID: 1233018)
- [Adobe ColdFusion] CAR Archive Directory Traversal (CVE-2025-43566) (Pattern ID: 1233019, 1233020)
- [XWiki] getdeleteddocuments.vm SQL Injection (CVE-2025-32429) (Pattern ID: 1233021)
- [Ivanti Endpoint Manager (Mobile)] SSHConfigImpl uploadPubKey Command Injection (CVE-2025-6770) (Pattern ID: 1233026)
- [Samsung MagicINFO 9 Server] FtpMetaUploadServlet doPost Directory Traversal (CVE-2025-54453) (Pattern ID: 1233027)
- [Nagios XI] Business Process Intelligence Arbitrary File Write (Pattern ID: 1233028, 1233029)
- [Apache OFBiz] Scrum Plugin Argument Injection (CVE-2025-54466) (Pattern ID: 1233031, 1233032)
- [Fortinet FortiWeb] get_fabric_user_by_token SQL Injection (CVE-2025-25257) (Pattern ID: 1233033)
- [Veeam Backup and Replication] Insecure Deserialization vulnerabilities (CVE-2025-23120, CVE-2025-23121) (Pattern ID: 1233034, 1233036)
- [WordPress] WPvivid Backup Plugin Arbitrary File Upload (CVE-2025-5961) (Pattern ID: 1233025)
- [Cisco Identity Services Engine] invokeStrongSwanShellScript Command Injection (CVE-2025-20281) (Pattern ID: 1233030, 1233037, 1233038, 1233039)
- [Allegra] Password Reset Authentication Bypass (CVE-2025-6216) (Pattern ID: 1233040)
- [CrushFTP] AS2 validation Authentication Bypass (CVE-2025-54309) (Pattern ID: 1233041)
- [Microsoft SharePoint Server] Exchange Calendar Overlay SSRF (CVE-2025-53760) (Pattern ID: 1233042, 1233043)
- [Microsoft Windows] WMPhoto setUniformTiling Heap Buffer Overflow (CVE-2025-29962) (Pattern ID: 1233044, 1233045, 1233046)
- [Netgate pfSense] Dashboard Widgets widgetkey XML Injection (CVE-2024-54779) (Pattern ID: 1233047)
- [Microsoft IIS Web Deploy] Remote Code Execution (CVE-2025-53772) (Pattern ID: 1233048)
- [ASUS] RT-AX55 Multiple Vulnerabilities (CVE-2023-39780) (Pattern ID: 1233049), RT-AC68U Command Injection (CVE-2018-20334) (Pattern ID: 1233050)
- [SonicWall SMA100] mod_httprrp.so Heap Buffer Overflow (CVE-2025-40597) (Pattern ID: 1233052), httpd __api__ Stack Buffer Overflow (CVE-2025-40596) (Pattern ID: 1233056)
- [JetBrains TeamCity] connectionEditParams DOM-based XSS (CVE-2025-52879) (Pattern ID: 1233053), favoritelcon Reflected XSS (CVE-2025-52876) (Pattern ID: 1233054)

Enhancements

N/A

Bugs Fixed

N/A

Changes

- The following IPS patterns have been modified or updated to improve system efficiency:
 - [ASUSWRT] LAN Backdoor Command Execution (CVE-2014-9583) (Pattern ID: 1130327)
 - [Cisco Identity Services Engine] enableStrongSwanTunnel Insecure Deserialization (CVE-2025-20337) (Pattern ID: 1233009)
 - [Microsoft SharePoint Server] ToolShell Unauthenticated Deserialization (CVE-2025-53770) (Pattern ID: 1232991)

Notes

- The following outdated or deprecated IPS patterns have been removed to improve system efficiency and focus on relevant threats:
 - [Cacti] Stored XSS (CVE-2024-43365) (Pattern ID: 1232741)
 - [Centreon] SQL Injection (CVE-2024-32501) (Pattern ID: 1232742)
 - [Ivanti Endpoint Manager] SQL Injection / Directory Traversal (CVE-2024-34785, CVE-2024-50322, CVE-2024-50330) (Pattern ID: 1232747, 1232855, 1232857)
 - [Ivanti Cloud Services] Command Injection (CVE-2024-47908) (Pattern ID: 1232877)
 - [Jenkins] Simple Queue Plugin XSS (CVE-2024-54003) (Pattern ID: 1232748)
 - [VMware vCenter] Out-of-bounds Write (CVE-2024-38812) (Pattern ID: 1232749)
 - [Mozilla] Animation Timeline UAF (CVE-2024-9680) (Pattern ID: 1232750)
 - [LibreNMS] XSS / Command Injection (CVE-2024-50352, CVE-2024-51092) (Pattern ID: 1232752, 1232730)
 - [Craft CMS] Code Injection (CVE-2024-56145) (Pattern ID: 1232755)
 - [Netgate pfSense] Stored XSS (CVE-2024-46538) (Pattern ID: 1232757)
 - [OpenSSL] DoS (CVE-2024-6119) (Pattern ID: 1232849)
 - [HPE Insight RS] XXE (CVE-2024-11622) (Pattern ID: 1232859)
 - [Rockwell ThinManager] Out-of-Bounds Read / Missing Authorization (CVE-2024-10386, CVE-2024-10387) (Pattern ID: 1232718, 1232720)
 - [Fortinet] FortiManager Command Injection (CVE-2024-47575) (Pattern ID: 1232721)
 - [Ivanti Avalanche] Directory Traversal (CVE-2024-47011) (Pattern ID: 1232726)
 - [MediaWiki] Path Traversal (CVE-2024-47841) (Pattern ID: 1232729)
 - [Grafana Labs Grafana] SQL Injection / LFI (CVE-2024-9264) (Pattern ID: 1232732)
 - [Palo Alto Networks PAN-OS] Auth Bypass / Command Injection (CVE-2024-0012, CVE-2024-9474) (Pattern ID: 1232734, 1232735)
 - [JetBrains TeamCity] Stored XSS (CVE-2024-47951) (Pattern ID: 1232736–1232739)
 - [Delta Electronics InfraSuite] Insecure Deserialization (CVE-2024-10456) (Pattern ID: 1232740)
 - [Gogs] Path Traversal (CVE-2024-55947) (Pattern ID: 1232867)



- [Fortinet FortiOS/FortiProxy] Auth Bypass (CVE-2024-55591) (Pattern ID: 1232874)
- [Progress WhatsUp Gold] SQL Injection (CVE-2024-46906) (Pattern ID: 1232875)
- [Rsync Daemon] Heap Buffer Overflow (CVE-2024-12084) (Pattern ID: 1232879)

Version: v13.0.25	Build: 25082518
Release Date: Sep 02, 2025	

Applicable Products

EDR-G9004 Series

Supported Operating Systems

N/A

New Features

- Added support for IPS pattern v1.146.
- [Apache Tomcat] HTTP Priority Header Denial of Service mitigated. (CVE-2025-31650) (Pattern ID: 1232959, 1232967)
- [Adobe Commerce / Magento] InputParamsResolver Improper Authorization vulnerabilities resolved. (CVE-2025-24434) (Pattern ID: 1232968–1232982)
- [Microsoft Windows] URL WorkingDirectory Directory Traversal (CVE-2025-33053) (Pattern ID: 1232984)
- [Microsoft Windows] Message Queuing Service Denial of Service (CVE-2023-28302) (Pattern ID: 1232983)
- [Microsoft Windows] Remote Desktop Gateway AuthS Denial of Service (CVE-2025-30394) (Pattern ID: 1232985, 1232986)
- [NodeBB] Stored Cross-Site Scripting in user profile 'About Me' section fixed. (CVE-2024-57041) (Pattern ID: 1232987)
- [SonicWall SMA100] download_tar Directory Traversal (CVE-2025-32819) (Pattern ID: 1232988)
- [SonicWall SMA100] General Directory Traversal (CVE-2025-32821) (Pattern ID: 1232965)
- [Microsoft SharePoint Server] ToolShell Unauthenticated Deserialization resolved. (CVE-2025-53770) (Pattern ID: 1232991)
- [Webmin] CGI xhr-get_autocompletes Command Injection patched. (CVE-2024-12828) (Pattern ID: 1232992)
- [Redis RedisBloom] Count-Min Sketch Integer Overflow protected. (CVE-2024-55656) (Pattern ID: 1232993, 1232995, 1232996)
- [ZendTo] dropoff tmp_name Directory Traversal vulnerability mitigated. (CVE-2025-34508) (Pattern ID: 1232997)
- [ISC BIND] Additional Section Handling Denial of Service fixed. (CVE-2024-11187) (Pattern ID: 1232989)
- [Ivanti Endpoint Manager] DownloadFile UniqueFilename Directory Traversal (CVE-2024-13171) (Pattern ID: 1232998, 1232999)
- [Ivanti Endpoint Manager] Mobile SSHConfigImpl uploadPubKey Command Injection (CVE-2025-6771) (Pattern ID: 1233008)
- [OpenEMR] Patient Demographics Additional Addresses Stored Cross-Site Scripting fixed. (CVE-2025-43860) (Pattern ID: 1233000, 1233004)
- [Rsync Daemon] Safe Links Handling Directory Traversal protected. (CVE-2024-12088) (Pattern ID: 1233001)
- [NI G Web Development Software] gwebproject ParseDataValueAsXmlHierarchy Insecure Deserialization mitigated. (CVE-2024-12742) (Pattern ID: 1233005, updated 1233005-1.1)
- [Adobe ColdFusion] System Probes Command Injection patched. (CVE-2025-43562) (Pattern ID: 1232994)
- [Wing FTP Server] Username Code Injection protected. (CVE-2025-47812) (Pattern ID: 1233002)
- [JetBrains TeamCity] Reflected Cross-Site Scripting vulnerabilities fixed in diskUsageBuildsStats.



(CVE-2025-52877) (Pattern ID: 1233007)

- [Cisco Identity Services Engine] enableStrongSwanTunnel Insecure Deserialization protected.

(CVE-2025-20337) (Pattern ID: 1233009)

- [WPS Office] Access via SSL enabled. (Pattern ID: 1165289, 1165290)
- [Hulu Media] Enhanced SSL media handling. (Pattern ID: 1165287, 1160111 updated)

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:
 - [Ivanti Cloud Services Appliance] removeCoreCertificate SQL Injection (CVE-2024-11773) (Pattern ID: 1232780, 1232781)
 - [Progress WhatsUp Gold] WriteDataFile Directory Traversal (CVE-2024-46909) (Pattern ID: 1232782)
 - [Ivanti Endpoint Manager] Directory Traversal & SQL Injection (CVE-2024-34787, CVE-2024-50326) (Pattern ID: 1232783, 1232790)
 - [Rockwell ThinManager] ThinServer.exe API Directory Traversal (CVE-2024-45826) (Pattern ID: 1232784)
 - [LibreNMS] Stored XSS & API Token vulnerabilities (CVE-2024-53457, CVE-2024-49754) (Pattern ID: 1232789, 1232796)
 - [Apache Traffic Control] SQL Injection (CVE-2024-45387) (Pattern ID: 1232794)
 - [Nagios XI] windows-winrm Command Injection (Pattern ID: 1232800)
 - [Zimbra Collaboration] Proxy Servlet SSRF (CVE-2024-45518) (Pattern ID: 1232798)
 - [Apache Solr] URL Path Authentication Bypass (CVE-2024-45216) (Pattern ID: 1232792)
 - [Microsoft Windows InternetShortcut] NTLM Relay (CVE-2025-21377) (Pattern ID: 1232817)
 - [HPE Insight Remote Support] XXE Injection (CVE-2024-53674) (Pattern ID: 1232815)
 - [Netgate pfSense] Stored XSS (CVE-2024-46538) (Pattern ID: 1232757)
 - [Zabbix] SQL Injection (CVE-2024-42327) (Pattern ID: 1232761)
 - [Centreon] SQL Injection (CVE-2024-55573) (Pattern ID: 1232821)
 - [Progress Kemp LoadMaster] Command Injection (CVE-2024-56131) (Pattern ID: 1232826)
 - [Fortinet FortiWeb] Command Injection (CVE-2024-50567) (Pattern ID: 1232827)
 - [WSO2 Multiple Products] SynapseArtifactUploaderAdmin Directory Traversal (CVE-2024-7074) (Pattern ID: 1232831)
 - [Legacy vulnerabilities] Old Adobe, Chrome, Windows SMB, Exim, HPE, Oracle, etc. (Pattern ID: 1134253–1134313, 1232623)



Version: v13.0.24	Build: 25072214
Release Date: Jul 31, 2025	

Applicable Products

EDR-G9004 Series

Supported Operating Systems

N/A

New Features

- Added support for IPS pattern v1.143.
- [Gladinet CentreStack] Hard-coded credentials vulnerability mitigated. (CVE-2025-30406) (Pattern ID: 1232951)
- [Grafana] DOM-based XSS vulnerability resolved in XY Chart. (CVE-2025-2703) (Pattern ID: 1232952)
- [Edimax Network Cameras] Command injection protection added. (CVE-2025-1316) (Pattern ID: 1232954)
- [XWiki] SQL injection vulnerability patched in query REST API. (CVE-2025-32969) (Pattern ID: 1232955)
- [Microsoft SharePoint Server] Unsafe reflection issue resolved. (CVE-2025-47163) (Pattern ID: 1232956)
- [Ivanti Products] Stack-based buffer overflow via X-Forwarded-For protected. (CVE-2025-22457) (Pattern ID: 1232957)
- [OpenEMR] Stored XSS in procedure order names fixed. (CVE-2025-32794) (Pattern ID: 1232960)
- [JetBrains TeamCity] Cross-site scripting vulnerabilities resolved. (CVE-2025-46618) (Pattern ID: 1232961–1232964)
- [SonicWall SMA100] Directory traversal protection added. (CVE-2025-32821) (Pattern ID: 1232965)
- [Citrix ADC (NetScaler)] Information disclosure vulnerability addressed. (CVE-2025-5777) (Pattern ID: 1232966)
- [WordPress Kubio AI Plugin] Local file inclusion protections added. (CVE-2025-2294) (Pattern ID: 1232969, 1232970)
- [NI FlexLogger] Directory traversal via URI file parsing mitigated. (CVE-2025-2449) (Pattern ID: 1232971)
- [Apache OFBiz] Stored XSS in Referer header resolved. (CVE-2025-30676) (Pattern ID: 1232972)
- [Ivanti MobileIron] Code injection defense added. (CVE-2025-4428) (Pattern ID: 1232973, 1232974)
- [Fortinet Products] Buffer overflow protection enforced. (CVE-2025-32756) (Pattern ID: 1232975)
- [Apache Tomcat] Denial of service via HTTP Priority Header mitigated. (CVE-2025-31650) (Pattern ID: 1232959, 1232967)
- [Adobe Commerce / Magento] Improper authorization vulnerabilities resolved. (CVE-2025-24434) (Pattern ID: 1232968, 1232976–1232982)
- [Microsoft Windows] Directory traversal protection on URL WorkingDirectory. (CVE-2025-33053) (Pattern ID: 1232984)
- [NodeBB] Stored XSS in user profile "About Me" section fixed. (CVE-2024-57041) (Pattern ID: 1232987)
- [SonicWall SMA100] download_tar directory traversal prevented. (CVE-2025-32819) (Pattern ID: 1232988)

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 SIP, OpenOffice.org, and Microsoft Office vulnerabilities (Pattern ID: 1051181, 1112770, 1130195)
 - ActiveX, GnuTLS, Adobe Flash, IIS WebDav, Tomcat JSP, Cacti, ksmbd, and others (Pattern ID: 1054716, 1057241, 1110011, 1110028, 1110042, 1112685, 1112761, 1232860, 1232866, 1232868)
 - Apache Solr, VMware HCX, SonicWall SSLVPN, and HPE Remote Support vulnerabilities (Pattern ID: 1232805, 1232809, 1232818, 1232825, 1232830, 1232848, 1232854)
 - Outdated patterns related to Ivanti, LibreNMS, Rockwell, Solr, WhatsUp Gold, and Nagios (Pattern ID: 1232780, 1232781, 1232782, 1232783, 1232784, 1232789, 1232790, 1232791, 1232792, 1232794, 1232796, 1232798, 1232800)

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

Applicable Products

EDR-G9004 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 ksmdb] 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-G9004 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-G9004 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-G9004 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-G9004 Series

Supported Operating Systems

N/A

New Features

- Added support for IPS pattern v1.102.

Enhancements

N/A

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-G9004 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

EDR-G9004 Series

Supported Operating Systems

N/A

New Features

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

Enhancements

N/A

Bugs Fixed

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

Changes

N/A

Notes

N/A