Network Security Package for EDR-G9004 Series Release Notes

Version: v19.0.13	Build: 26102715
Release Date: Oct 30, 2026	

Applicable Products

EDR-G9004 Series

Supported Operating Systems

N/A

New Features

• Added support for IPS pattern v1.209.
• [HMA VPN] TCP access classification signature added. (Pattern ID: 1164949)
• [Midjourney] SSL access classification signature added. (Pattern ID: 1165293)
• [Cisco Identity Services Engine] uploadPartialSyncFiles directory traversal vulnerability mitigated. (CVE-2026-20180) (Pattern ID: 1233497)
• [Fortinet FortiSandbox] Cron Job command injection vulnerability mitigated. (CVE-2026-84387) (Pattern ID: 1233502)
• [Zoho ManageEngine Password Manager Pro] checkQuery SQL injection vulnerability mitigated. (CVE-2026-11840) (Pattern ID: 1233504)
• [Microsoft SharePoint Server] DLPPolicyDefinition reflected XSS vulnerability mitigated. (CVE-2026-20959) (Pattern ID: 1233509)
• [Citrix ADC (NetScaler)] Remote code execution vulnerability mitigated. (CVE-2026-88771) (Pattern ID: 1233512)
• [Cisco Secure FMC Software] External database access insecure deserialization vulnerability mitigated. (CVE-2026-20242) (Pattern ID: 1233519)
• [Meowdoku] SSL access classification signature added. (Pattern ID: 1165368)
• [Fortinet FortiSandbox] tracer_behavior command injection vulnerability mitigated. (CVE-2026-39808) (Pattern ID: 1233534)
• [Fortinet FortiMail] ibe directory traversal vulnerability mitigated. (CVE-2026-104286) (Pattern ID: 1233537)
• [WordPress] WP_Query SQL injection vulnerability mitigated. (CVE-2026-60137) (Pattern ID: 1233541)
• [PHP] Session stale global state use-after-free vulnerability mitigated. (CVE-2026-109619) (Pattern ID: 1233546, 1233547, 1233548, 1233550)

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• The following outdated or deprecated IPS patterns have been removed to improve system efficiency and focus on relevant threats:
  • [Progress Kemp Flowmon] ConfluencePresenter.php command injection vulnerability (CVE-2024-2389) (Pattern ID: 1232433, 1232434, 1232435)
  • [XWiki] UIExtension WikiUIExtensionParameters code injection vulnerability (CVE-2024-31997)

(Pattern ID: 1232429)
- [Mozilla PDF.js] Arbitrary FontRenderer JavaScript remote code execution vulnerability (CVE-2024-4367) (Pattern ID: 1232431)
- [Zabbix] Audit Log SQL injection vulnerability (CVE-2024-22120) (Pattern ID: 1232432)
- [JetBrains TeamCity] JspPrecompilation authentication bypass vulnerability (CVE-2024-23917) (Pattern ID: 1232424)
- [Ivanti Avalanche] getAdhocFilePath directory traversal vulnerability (CVE-2024-24992) (Pattern ID: 1232428)
- [SolarWinds Access Rights Manager] JsonSerializationBinder insecure deserialization vulnerability (CVE-2024-23478) (Pattern ID: 1232415)
- [Delta Industrial Automation DIAEnergie] Handler_CFG.ashx SQL injection vulnerability (CVE-2024-28891) (Pattern ID: 1232417)
- [Mura CMS] SQL injection vulnerability (CVE-2024-32640) (Pattern ID: 1232421)
- [XWiki] Solr Space Facet code injection vulnerability (CVE-2024-31984) (Pattern ID: 1232422)
- [Cacti] cmd_realtime.php command injection vulnerability (CVE-2024-29895) (Pattern ID: 1232423)

Version: v17.0.17	Build: 26042414
Release Date: May 13, 2026	

Applicable Products

EDR-G9004 Series

Supported Operating Systems

N/A

New Features

• Added support for IPS pattern v1.182.
• [Apache httpd] NTLM relay vulnerability mitigated (CVE-2025-59775) (Pattern ID: 1233258)
• [JetBrains TeamCity] Reflected cross-site scripting vulnerability mitigated (CVE-2025-68165) (Pattern ID: 1233261)
• [OpenEMR] Stored cross-site scripting vulnerability mitigated (CVE-2025-69231) (Pattern ID: 1233262, 1233263)
• [Cisco Secure FMC Software] Authentication bypass vulnerability mitigated (CVE-2026-20079) (Pattern ID: 1233264)
• [MLflow Tracking Server] Path traversal vulnerability mitigated (CVE-2025-11201) (Pattern ID: 1233265, 1233266)
• [Microsoft Windows] desktop.ini NTLM relay vulnerability mitigated (CVE-2026-20872) (Pattern ID: 1233267)
• [Langflow-AI] Code injection vulnerability mitigated (CVE-2026-33017) (Pattern ID: 1233268)
• [LibreNMS] SQL injection vulnerability mitigated (CVE-2026-26988) (Pattern ID: 1233269, 1233270)
• [Apache Tomcat] Remote code execution vulnerability mitigated (CVE-2024-56337) (Pattern ID: 1233273)
• [VOIP Applications] FaceTime communication classification signature added (Pattern ID: 1165318)

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

• The following outdated or depreciated IPS patterns have been removed to improve system efficiency and focus on relevant threats:
  • [GitLab Community and Enterprise Edition] Markdown render denial-of-service vulnerability (CVE-2024-2651) (Pattern ID: 1232522)
  • [Apache NiFi] Stored cross-site scripting vulnerability (CVE-2024-37389) (Pattern ID: 1232523)
  • [Provectus UI for Apache Kafka] Insecure deserialization vulnerability (CVE-2024-32030) (Pattern ID: 1232520)
  • [Cacti] SQL injection vulnerability (CVE-2024-31458) (Pattern ID: 1232521)
  • [Rejetto HTTP File Server] Command injection vulnerability (CVE-2024-39943) (Pattern ID: 1232516)
  • [GeoServer / GeoTools] Remote code execution vulnerability (CVE-2024-36401) (Pattern ID: 1232505, 1232510)
  • [Progress MOVEit Transfer] Authentication bypass vulnerability (CVE-2024-5806) (Pattern ID: 1232506, 1232507)
  • [Apache OFBiz] Directory traversal vulnerability (CVE-2024-36104) (Pattern ID: 1232508)
  • [Centreon] SQL injection vulnerability (CVE-2024-23118) (Pattern ID: 1232509)

- [Apache JSPWiki] Stored cross-site scripting vulnerability (CVE-2024-27136) (Pattern ID: 1232514)

Version: v17.0.15	Build: 26032517
Release Date: Apr 15, 2026	

Applicable Products

EDR-G9004 Series

Supported Operating Systems

N/A

New Features

• Added support for IPS pattern v1.178.
• [Fortinet FortiSandbox] Reflected cross-site scripting vulnerability mitigated (CVE-2025-54353) (Pattern ID: 1233221)
• [Centreon] Command injection vulnerability mitigated (CVE-2025-5965) (Pattern ID: 1233222, 1233225)
• [Microsoft Windows NetLogon RPC] Denial-of-service vulnerability mitigated (CVE-2025-49716) (Pattern ID: 1233226)
• [Netgate pfSense Suricata] Stored cross-site scripting vulnerability mitigated (CVE-2025-34177) (Pattern ID: 1233227, 1233228)
• [LibreNMS] Stored cross-site scripting vulnerability mitigated (CVE-2025-62412) (Pattern ID: 1233229, 1233231, 1233232)
• [Zoho ManageEngine Analytics Plus] SQL injection vulnerability mitigated (CVE-2025-9428) (Pattern ID: 1233230)
• [Fortinet FortiClient EMS] SQL injection vulnerability mitigated (CVE-2025-59922) (Pattern ID: 1233234)
• [Siemens SINEC NMS] Directory traversal vulnerabilities mitigated (CVE-2025-40737, CVE-2025-40738) (Pattern ID: 1233238, 1233237)
• [Fortinet FortiSandbox] Reflected cross-site scripting vulnerability mitigated (CVE-2025-52436) (Pattern ID: 1233239)
• [Cisco Multiple Products] Buffer overflow vulnerability mitigated (CVE-2025-20333) (Pattern ID: 1233240)
• [Ivanti Endpoint Manager Mobile] Code injection vulnerability mitigated (CVE-2026-1340) (Pattern ID: 1233210)
• [Zimbra Collaboration] Local file inclusion vulnerability mitigated (CVE-2025-68645) (Pattern ID: 1233235, 1233236)
• [WordPress WP Statistics Plugin] Stored cross-site scripting vulnerability mitigated (CVE-2025-9816) (Pattern ID: 1233241, 1233242)
• [Ivanti Endpoint Manager] Authentication bypass vulnerability mitigated (CVE-2026-1603) (Pattern ID: 1233244)
• [Cisco Identity Services Engine] Reflected cross-site scripting vulnerability mitigated (CVE-2025-20303) (Pattern ID: 1233247)
• [Cisco Multiple Products] Authentication bypass vulnerability mitigated (CVE-2025-20362) (Pattern ID: 1233251)
• [Fortinet FortiWeb] Authentication bypass vulnerability mitigated (CVE-2025-64447) (Pattern ID: 1233254)
• [Microsoft SharePoint] Insecure deserialization vulnerability mitigated (CVE-2025-49712) (Pattern ID: 1233252)
• [Zoho ManageEngine ADSelfService Plus] SQL injection vulnerability mitigated (CVE-2026-1367) (Pattern ID: 1233255)
• [OpenEMR] SQL injection vulnerability mitigated (CVE-2026-25746) (Pattern ID: 1233257)
• [AI Applications] Grok access classification signatures added (Pattern ID: 1165302)
• [AI Applications] NotebookLM access classification signatures added (Pattern ID: 1165303)

• [Media Applications] BBC iPlayer access classification signatures added (Pattern ID: 1165308, 1165309, 1165310, 1165311, 1165312)

Enhancements

N/A

Bugs Fixed

N/A

Changes

• The following IPS patterns have been modified or updated to improve system efficiency:
• [Netgate pfSense Suricata] Stored cross-site scripting detection signature updated (CVE-2025-34177) (Pattern ID: 1233106, 1233107)
• [Netgate pfSense Suricata] Directory traversal detection signature updated (CVE-2025-12490) (Pattern ID: 1233155, 1233156)

Notes

• The following outdated or deprecated IPS patterns have been removed to improve system efficiency and focus on relevant threats:
• [Progress WhatsUp Gold] Denial-of-service vulnerability (CVE-2024-5011) (Pattern ID: 1232542, 1232541)
• [Dolibarr ERP and CRM] Cross-site scripting vulnerability (CVE-2024-34051) (Pattern ID: 1232543)
• [WordPress SEO Plugin] SQL injection vulnerability (CVE-2024-6497) (Pattern ID: 1232549)
• [Apache Superset] Arbitrary file read vulnerability (CVE-2024-34693) (Pattern ID: 1232550)
• [LibreNMS] SQL injection vulnerability (CVE-2024-32480) (Pattern ID: 1232554)
• [Cacti] Stored cross-site scripting vulnerability (CVE-2024-31444) (Pattern ID: 1232555)
• [Apache OFBiz] Directory traversal vulnerability (CVE-2024-32113) (Pattern ID: 1232556, 1232560)
• [Apache OFBiz] Remote code execution vulnerability (CVE-2024-36104) (Pattern ID: 1232562)
• [Progress WhatsUp Gold] Directory traversal vulnerability (CVE-2024-4885) (Pattern ID: 1232566)
• [GitLab] Denial-of-service vulnerability (CVE-2024-2874) (Pattern ID: 1232570)
• [PaperCut NG/NF] Authentication bypass vulnerability (CVE-2024-1222) (Pattern ID: 1232572)
• [VMware vCenter Server] Integer underflow vulnerability (CVE-2024-37079) (Pattern ID: 1232575)
• [Logsign Unified SecOps Platform] Missing authentication vulnerability (CVE-2024-5721) (Pattern ID: 1232576)
• [ServiceNow] Jelly template injection vulnerability (CVE-2024-4879) (Pattern ID: 1232524)
• [Fortra FileCatalyst Workflow] SQL injection vulnerability (CVE-2024-5276) (Pattern ID: 1232525)
• [Progress WhatsUp Gold] Unrestricted file upload vulnerability (CVE-2024-4884) (Pattern ID: 1232526)

Version: v15.0.20	Build: 25121116
Release Date: Dec 15, 2025	

Applicable Products

EDR-G9004 Series

Supported Operating Systems

N/A

New Features

• Added support for IPS pattern v1.160.
• [JetBrains TeamCity] Reflected XSS in agentpushPreset.html (CVE-2025-54534) (Pattern ID: 1233096)
• [Oracle E-Business Suite] SSRF in Configurator (CVE-2025-61884) (Pattern ID: 1233098, 1233099)
• [FlowiseAI] Forgot Password Auth Bypass (CVE-2025-58434) (Pattern ID: 1233100)
• [Netgate pfSense] Stored XSS in Status_Traffic_Totals (CVE-2025-34174) (Pattern ID: 1233101)
• [JetBrains TeamCity] DOM-based XSS in checksTrigger (CVE-2025-47851) (Pattern ID: 1233097, 1233102, 1233103, 1233104)
• [pfSense Suricata] Stored XSS in policy_name (CVE-2025-34177) (Pattern ID: 1233106, 1233107)
• [Nagios XI] Multiple Wizards Command Injection (CVE-2025-34227) (Pattern ID: 1233109)
• [Advantech iView] Directory Traversal in processImportRequest (CVE-2025-46704) (Pattern ID: 1233111)
• [Apache Kylin] Authentication Bypass (CVE-2025-61733) (Pattern ID: 1233112)
• [Zabbix] Visible Name SQL Injection (CVE-2025-27240) (Pattern ID: 1233108, 1233116)
• [Samsung MagicINFO] File Upload Vulnerabilities (CVE-2025-54441, CVE-2025-54442) (Pattern ID: 1233118, 1233120)
• [Samsung MagicINFO] XXE in parseXMLString (CVE-2025-54445) (Pattern ID: 1233124)
• [Vim] tar.vim Command Injection (CVE-2025-27423) (Pattern ID: 1233125)
• [LibreNMS] Alert Transport Stored XSS (CVE-2025-62411) (Pattern ID: 1233126)
• [Ivanti Endpoint Manager] PatchSourceIO Arbitrary File Upload (CVE-2025-9872) (Pattern ID: 1233130, 1233131, 1233132)
• [ChatGPT Access] AI traffic classification signatures (Pattern ID: 1165027, 1165029, 1165030, 1165037, 1165263)

Enhancements

N/A

Bugs Fixed

• Incorrect asset recognition due to unused SNMP port query.
• The system freezes when enabling or updating Asset Recognition.
• CPU load is abnormally high after updating the Security Package.

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] Authentication Bypass / Command Injection (Pattern ID: 1232688, 1232691)
  - [SuiteCRM] Delegate SQL Injection (Pattern ID: 1232690)
  - [GitLab] OAuth XSS & SAML Authentication Bypass (Pattern ID: 1232695, 1232680)
  - [Palo Alto Networks Expedition] Command Injection & SQL Injection (Pattern ID: 1232696, 1232677)

- [Zoho ManageEngine] URL Monitoring SQL Injection (Pattern ID: 1232685)
- [Cacti] Arbitrary File Read / Write (Pattern ID: 1232922, 1232676)
- [Fortinet FortiSandbox] Multiple Vulnerabilities (Pattern ID: 1232925, 1232934, 1232935)
- [Ivanti Avalanche] SecureFilter Auth Bypass (Pattern ID: 1232931)
- [Zabbix] SQL Injection (Pattern ID: 1232933)
- [Kemp LoadMaster] Command Injection (Pattern ID: 1232938, 1232939, 1232940)
- [Ivanti Endpoint Manager] NTLM Relay & SQL Injection (Pattern ID: 1232941, 1232679)
- [WhatsUp Gold] Information Disclosure (Pattern ID: 1232673)
- [Jenkins] Arbitrary File Read (Pattern ID: 1232678)

Version: v15.0.18	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: v13.0.24	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] 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-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