



CylanceMDR

Release Notes

August 2024

Contents

- What's new in CylanceMDR..... 4**
- Fixed issues..... 5**
- Known issues..... 6**
- CylanceMDR protection enhancements..... 7**
 - Previous CylanceMDR protection enhancements.....8
- Legal notice..... 15**

What's new in CylanceMDR

What's new in the August 2024 update

CylanceMDR Pro: The CylanceMDR Pro subscription is a fully-featured option that includes the same features as CylanceMDR Advanced, plus the option to use non-Cylance products for alert reporting and the integration of third-party log sources such as for firewall capabilities. If you choose to use Cylance products such as CylancePROTECT and CylanceOPTICS, CylanceMDR onboarding specialists will assist with their configuration.

For more information, see the [CylanceMDR overview](#).

What's new in the May 2024 update

- **New product name:** CylanceGUARD is now known as CylanceMDR.
- **CylanceMDR On-Demand:** The CylanceMDR On-Demand subscription is a convenient and helpful option if your organization monitors the alerts that are reported to the Cylance console. With this subscription, you can request CylanceMDR support on demand for any alerts that you think might be a threat but you need the time and expertise of a CylanceMDR analyst to help you resolve it. You can request support from an alert group in the Alerts view in the Cylance management console. CylanceMDR analysts are immediately notified with the alert details and can start their investigation and assess the threat. To follow up on the investigation (for example, to share additional details), you can log in to the CylanceMDR (CylanceGUARD) portal and find the alert in the Escalations screen.

If you want to have dedicated CylanceMDR analysts monitoring alerts for you 24x7, consider the CylanceMDR Standard and CylanceMDR Advanced subscriptions. For more information, see the [CylanceMDR overview](#).

Fixed issues

August 2024 update

There were no fixed issues in this release.

May 2024 update

There were no fixed issues in this release.

Known issues

When trying to request on-demand assistance from the Cylance console for CylanceMDR, a "The CylanceMDR Support request could not be sent" error message appears if your CylanceMDR On Demand account setup has not been completed. Contact BlackBerry Support to complete the setup. (UES-17028)

CylanceMDR protection enhancements

Due to some emerging threats, CylanceMDR has implemented the following CylanceOPTICS rules for improved security and telemetry for analysts. These rules are already in effect and no further action is required from your organization.

Latest enhancements (May and June 2024)

Threat or vulnerability	Description
Updated rule for advanced detection of Powershell scheduled task creation via Windows Script Host	<ul style="list-style-type: none">• Rule Name: "Powershell Scheduled Task Creation via Windows Script Host"• MITRE Techniques: T1053, T1053.005, T1059, T1059.001, T1059.007• Description: This rule detects the creation of a scheduled task via Powershell executed by a suspicious JavaScript/JScript file. This attack chain is highly suspicious and is also indicative of GootLoader activity.• Platform: Windows• Additional reference: BlackBerry Blogs, Red Canary• Date added: June 2024
Updated rule for advanced detection of the execution of an 8-character temporary file created by svchost	<ul style="list-style-type: none">• Rule Name: "8 Character Temp File Created by Svchost"• MITRE Techniques: T1074, T1074.001• Description: This rule detects the creation of temporary files via svchost within critical Windows system directories, such as Windows/System32 and Temp. Such activity often indicates potential malware or unauthorized software attempting to execute or persist on the system.• Platform: Windows• Additional reference: Clearsky, Microsoft• Date added: June 2024
Updated rule for advanced detection of the execution of a Stager payload from PowerShell Empire	<ul style="list-style-type: none">• Rule Name: "PowerShell Empire Stager Payload Executed"• MITRE Techniques: T1059, T1059.001, T1071, T1071.001• Description: This rule detects the execution of a Stager related to Powershell Empire command and control activity. The rule pays attention to commonly used web requests such as /admin/get.php, /admin/news.php, and /login/process.php. PowerShell Empire is a post-exploitation framework used by security professionals and hackers to facilitate remote access and control of compromised systems through PowerShell scripts.• Platform: Windows• Additional reference: Red Team Notes• Date added: May 2024

Threat or vulnerability	Description
Updated rule for advanced detection of the Csvde.exe export command	<ul style="list-style-type: none"> • Rule Name: "Csvde.exe Export Command" • MITRE Techniques: T1087, T1069, T1018, T1087.002, T1119 • Description: This rule detects the use of Csvde.exe for export data. Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifiers on a network that may be used for lateral movement from the current system. Cloud environments typically provide easily accessible interfaces to obtain user lists. On hosts, adversaries can use command line functionality to identify accounts. • Platform: Windows • Additional reference: MITRE • Date added: May 2024
Updated rule for advanced detection of local credential dump from NTDS, SAM or LSA using SecretsDump	<ul style="list-style-type: none"> • Rule Name: "Local Credential Dump from NTDS, SAM or LSA via SecretsDump" • MITRE Techniques: T1003, T1003.002, T1003.003, T1003.004, T1059, T1059.006 • Description: Adversaries may attempt to steal credential information from the NTDS file (%SystemRoot%\NTDS\Ntlds.dit) or from the Windows Registry hives which store the Security Account Manager (SAM) database and Local Security Authority (LSA) secrets. This rule detects the usage of a tool called secretsdump.py, which can be used to locally dump the credential information like domain hashes from the NTDS.dit file, SAM, and LSA secrets from the exported registry hives. • Platform: Windows • Additional reference: Hacker Recipes NTDS, Hacker Recpies SAM & LSA • Date added: May 2024
Updated rule for advanced detection of a remote credential dump from the registry hive	<ul style="list-style-type: none"> • Rule Name: "Remote Credential Dump from Registry Hive" • MITRE Techniques: T1003, T1003.002 • Description: This rule detects a Logon Type 3 event, a 'Remote Registry Service' start, and the creation of 8-character .tmp files. These are indicative of a credential dump from the registry. Threat actors can use tools like impacket to query the registry hive remotely, dump the SAM and SYSTEM hives into memory, and exfiltrate to a C2 Server. Verify user login activity and any network connections to internal/external hosts to determine if activity is malicious. • Platform: Windows • Additional reference: Medium • Date added: May 2024

Previous CylanceMDR protection enhancements

Due to some emerging threats, CylanceMDR has implemented the following CylanceOPTICS rules for improved security and telemetry for analysts. These rules are already in effect and no further action is required from your organization. To see the newest CylanceMDR rules, see [CylanceMDR protection enhancements](#).

Threat or vulnerability	Description
Updated rule for enhanced investigation of system information discovery through service enumeration	<ul style="list-style-type: none"> • Rule Name: "System Information Discovery via Service Enumeration" • MITRE Techniques: T1082, T1007 • Description: This rule detects registered local system services usage of 'tasklist /svc', or 'net start' by a non-administrator user. Adversaries may obtain information about services using tools as well as OS utility commands. Adversaries may use the commands to get a list of the services on the system. • Platform: Windows • Additional reference: MITRE • Date added: April 2024
Updated rule for advanced detection of the extraction of the domain database (including password hashes) using ntdsutil.exe	<ul style="list-style-type: none"> • Rule Name: "Domain Database including Password Hashes Extracted via ntdsutil.exe" • MITRE Techniques: T1003, T1003.003 • Description: Adversaries may attempt to access or create a copy of the Active Directory (AD) domain database to steal credential information, as well as obtain other information about domain members such as devices, users, groups, and access rights. By default, the NTDS file is located in %SystemRoot%\NTDS\Ntds.dit of a domain controller. This rule detects the use of the built-in Windows tool, ntdsutil.exe, to extract a copy of the AD domain database (which includes the password hashes for all the users of the domain). Hashes can then be exfiltrated from the host and be used for brute force attacks offline. • Platform: Windows • Additional reference: MITRE • Date added: April 2024
Updated rule for advanced detection of enumeration of browser bookmarks	<ul style="list-style-type: none"> • Rule Name: "Enumeration of Browser Bookmarks" • MITRE Techniques: T1217, T1555, T1555.003 • Description: This rule detects the enumeration or discovery of web browser bookmark database files. Adversaries may enumerate browser bookmarks to discover more information about a compromised host. Browser bookmarks can show a user's personal information and information about internal network resources. • Platform: Linux • Additional reference: MITRE • Date added: April 2024
Updated rule for advanced detection of Windows Defender registry key modification	<ul style="list-style-type: none"> • Rule Name: "Windows Defender Registry Key Modifications" • MITRE Techniques: T1562, T1562.001, T1112 • Description: This rule detects the modification of Windows Defender registry keys, which may be used to disable or modify security tools. • Platform: Windows • Additional reference: MITRE • Date added: April 2024

Threat or vulnerability	Description
Updated rule for enhanced investigation of account or group discovery via dscl	<ul style="list-style-type: none"> • Rule Name: "Account or Group Discovery via dscl" • MITRE Techniques: T1069.002, T1087, T1087.001, T1087.002 • Description: This rule detects evidence of account or group discovery, according to MITRE techniques T1087 and T1069. • Platform: macOS • Additional reference: MITRE T1087, MITRE T1069 • Date added: April 2024
Updated rule for enhanced investigation of file and directory discovery through the Windows command line	<ul style="list-style-type: none"> • Rule Name: "File and Directory Discovery via Cmd" • MITRE Techniques: T1083 • Description: This rule detects file and directory discovery through the Windows command line (cmd). Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. • Platform: Windows • Additional reference: MITRE • Date added: April 2024
Updated rule for advanced detection of the ScreenConnect authentication bypass vulnerability CVE-2024-1709	<ul style="list-style-type: none"> • Rule Name: "ScreenConnect Authentication Bypass Vulnerability CVE-2024-1709" • MITRE Techniques: T1556 • Description: This rule detects potential activities associated with the successful exploitation of CVE-2024-1709. • Platform: Windows • Additional reference: Huntress • Date added: April 2024
Updated rule for advanced detection of payload creation via compiled HTML (.chm) file	<ul style="list-style-type: none"> • Rule Name: "Payload Creation Via Compiled HTML (CHM) File" • MITRE Techniques: T1218, T1218.001 • Description: This rule detects the creation of a possible payload like script or executable via compiled HTML files (.chm) loaded by the HTML Help executable program (hh.exe). CHM files are compressed compilations of various content such as HTML documents, images, and scripting/web related programming languages such VBA, JScript, Java, and ActiveX. Adversaries may abuse CHM files to conceal malicious code. Legitimate software may execute CHM files. • Platform: Windows • Additional reference: Lookout • Date added: March 2024 (update)

Threat or vulnerability	Description
<p>Updated rule for advanced detection of payload execution from Appdata\Local\Temp Directory</p>	<ul style="list-style-type: none"> • Rule Name: "Payload Execution from Appdata Local Temp Directory" • MITRE Techniques: T1059, T1059.003 • Description: This rule detects the execution of scripts and executables from the AppData\Local\Temp directory via Windows Command Shell (cmd.exe). It is common for legitimate software to execute from this directory as well. Analysis of the script or executable is necessary to determine if it is being weaponized by a threat actor. • Platform: Windows • Additional reference: MITRE • Date added: March 2024
<p>Updated rule for advanced detection of Windows Defender service shutdown via net.exe</p>	<ul style="list-style-type: none"> • Rule Name: "Windows Defender Service Shutdown via net.exe" • MITRE Techniques: T1562, T1562.001, T1489 • Description: This rule detects if the Windows Defender service was terminated using net.exe. Adversaries may modify and/or disable security tools to avoid possible detection of their malware tools and activities. This may take many forms, such as killing security software processes or services. • Platform: Windows • Additional reference: MITRE • Date added: March 2024
<p>Updated rule for advanced detection of port forwarding SSH tunnel command execution</p>	<ul style="list-style-type: none"> • Rule Name: "Port Forwarding SSH Tunnel Command Execution" • MITRE Technique: T1572, T1021, T1021.004 • Description: This rule detects when SSH is executed using the <i>-N</i> and <i>-R</i> flags. These arguments are used to create port forwarding to a C2 server via an SSH tunnel. Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection or network filtering, and/or enable access to otherwise unreachable systems. The outbound IP address should be analyzed to determine false positives. • Platform: Windows • Additional reference: Medium • Date added: March 2024
<p>Updated rule for advanced detection of Windows Defender Antivirus Engine restored to default settings</p>	<ul style="list-style-type: none"> • Rule Name: "Windows Defender Antivirus Engine Restored to Default" • MITRE Technique: T1562, T1562.001 • Description: This rule detects attempts to restore Windows Defender to the original default settings. Adversaries may modify and/or disable security tools to avoid possible detection of their malware tools and activities. Adversaries may also tamper with artifacts deployed and utilized by security tools. • Platform: Windows • Additional reference: MITRE • Date added: March 2024

Threat or vulnerability	Description
Updated rule for advanced detection of obfuscated Bash History deletion	<ul style="list-style-type: none"> • Rule Name: “Bash History Deletion” • MITRE Technique: T1070, T1070.003 • Description: This rule detects the deletion of the bash_history file, which keeps track of the commands that users entered on the command line. An adversary may clear the command history of a compromised account to conceal the actions undertaken during an intrusion. • Platform: macOS • Additional reference: MITRE • Date added: March 2024
Updated rule for advanced detection of Bash History modification and deletion	<ul style="list-style-type: none"> • Rule Name: “Bash History Modification & Deletion” • MITRE Technique: T1552, T1552.003, T1070, T1070.003 • Description: This rule detects the modification or deletion of the bash_history file. Bash keeps track of the commands that users entered on the command line with the 'history' utility. Users often enter usernames and passwords on the command line as parameters to programs, which are then saved to this file when they log out. Adversaries can abuse this by looking through the file for potential credentials. • Platform: macOS • Date added: November 2023
Updated rule for advanced detection of critical Cylance binaries moved	<ul style="list-style-type: none"> • Rule Name: “Critical Cylance Binaries Moved” • Description: This rule detects when CyOptics.exe, CylanceSvc.exe, and CyProtect.exe are being moved to a different directory. Adversaries may try to move the Cylance files to bypass Cylance protection and to avoid detection of their malware, tools, and activities. False positives are likely with file backup and synchronization software. • Platform: Windows • Date added: November 2023
Updated rule for advanced detection of process execution via compiled HTML (.chm) file	<ul style="list-style-type: none"> • Rule Name: “Process Execution Via Compiled HTML (CHM) File” • Description: This rule detects the execution of a process via compiled HTML files (.chm) loaded by the HTML Help executable program (hh.exe). CHM files are compressed compilations of various content such as HTML documents, images, and scripting or web-related programming languages such as VBA, JScript, Java, and ActiveX. Adversaries may abuse CHM files to conceal malicious code. Legitimate software may execute CHM files. • Platform: Windows • Additional reference: Lookout • Date added: November 2023

Threat or vulnerability	Description
<p>Updated rule for advanced detection of Svchost launching Rundll32 via scheduled task</p>	<ul style="list-style-type: none"> • Rule Name: "Svchost Schedule Task Launches Rundll32" • MITRE Technique: T1053.005, T1218.011 • Description: This rule detects the execution of rundll32.exe through a scheduled task. Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious rundll32 exploitation. False positives are likely with legitimate software and Windows services. • Platform: Windows • Additional reference: Medium • Date added: November 2023
<p>Updated rule for advanced detection of debugger registry value modification for accessibility features</p>	<ul style="list-style-type: none"> • Rule Name: "Debugger Registry Value Modification for Accessibility Features" • Description: This rule detects when a registry value for Windows accessibility features has been modified to launch another program as a debugger. Windows contains accessibility features that may be launched with a key combination before a user has logged in, such as when the user is on the Windows login screen. Adversaries can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system. This can be done by using Image File Execution Options (IFEO) which enables developers to attach a debugger to an application that can be used to intercept calls to the application executable. There is no validation of whether the program listed as a debugger in the registry is legitimately a debugger, so malicious actors can leverage this to execute arbitrary payloads when specific applications (for example, sethc.exe) are executed. • Platform: Windows • Additional reference: Red Team Notes • Date added: November 2023
<p>Updated rule for advanced detection of obfuscated Base64 decoding method executed via PowerShell</p>	<ul style="list-style-type: none"> • Rule Name: "Obfuscated Base64 Decoding Method Executed via PowerShell" • MITRE Technique: T1059.001, T1027.010 • Description: This rule detects the execution of an obfuscated 'frombase64string' method in a PowerShell payload. Adversaries can obfuscate this method by reversing the string to evade detection. This technique is most commonly associated with malware generated from the BatCloak engine. False positives are not likely. De-obfuscation of the command line is required to determine the impact. • Platform: Windows • Additional reference: SANS • Date added: November 2023

Threat or vulnerability	Description
<p>Updated rule for advanced detection of UAC Bypass via fodhelper.exe activity</p>	<ul style="list-style-type: none"> • Rule Name: "UAC Bypass via Fodhelper.exe" • MITRE Technique: T1548.002 • Description: This rule detects a privilege escalation technique of bypassing UAC using PowerShell to modify registry keys for fodhelper.exe. Adversaries exploit this bypass to launch malware with administrative privileges. False positives are not likely. • Platform: Windows • Additional reference: Penetration Testing Lab • Date added: November 2023
<p>Updated rule for advanced detection of payload creation via compiled HTML (CHM) file</p>	<ul style="list-style-type: none"> • Rule Name: "Payload Creation Via Compiled HTML (CHM) File " • MITRE Technique: T1218, T1218.001 • Description: This rule detects the creation of a possible payload like a script or executable via compiled HTML files (.chm) loaded by the HTML Help executable program (hh.exe). CHM files are compressed compilations of various content such as HTML documents, images, and scripting or web-related programming languages such VBA, JScript, Java, and ActiveX. Adversaries may abuse CHM files to conceal malicious code. Legitimate software may execute CHM files. • Platform: Windows • Additional reference: Lookout • Date added: November 2023

Legal notice

©2024 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

Use of this BlackBerry product and/or service is governed by a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY SUCH WRITTEN AGREEMENTS OR OTHER WARRANTIES PROVIDED BY BLACKBERRY.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at <http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp>.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada