CylanceMDR

Release Notes

March 2025

Contents

What's new in CylanceMDR

What's new in the February 2025 update

Advanced detection and engagement: The CylanceMDR team can now leverage the MDR platform to engage customers more proactively about threats as required, based on advanced findings from threat hunting investigations.

What's new in the January 2025 update

AI-powered Cylance Assistant for CylanceMDR incidents: In the Incidents view, you can use the AI-powered Cylance Assistant when viewing the details of a triggering alert to provide a summary analysis of instigating processes or targeting processes (for example, a command line execution). The Cylance Assistant leverages rich cybersecurity knowledge sources to provide valuable information to aid you in your threat investigations. You can copy the analysis to a clipboard.

What's new in the October 2024 update (Unified console)

Unified CylanceMDR console: The CylanceMDR console is now unified with the Cylance console, which streamlines the management of your devices running CylancePROTECT, CylanceOPTICS and CylanceGATEWAY with CylanceMDR. In the Cylance console, you can manage CylanceMDR escalations seamlessly and communicate with the CylanceMDR team from a single console.

The key features of the unified console are:

- Manage all your Cylance devices and CylanceMDR escalations from one place.
- Simplified user experience for easy management of escalation workflows and collaboration.
- Use the same username and password as the Cylance console for easier access.

Note: Current CylanceMDR (formerly CylanceGUARD) tenants in the non-unified portal will be progressively migrated to the unified console. If you are using the non-unified portal, you will receive a notification from BlackBerry indicating the migration date and links to webinars and documentation. Open escalations in the non-unified portal will not be migrated to the unified console, but they will remain in the portal where they can be closed. Devices that are managed in the Cylance console will not be impacted.

The premigration user guide for the non-unified portal is available separately with the latest CylanceMDR documentation.

Fixed issues

December 2024

On the Incidents page of the Cylance console, the assignee field of an escalated incident appeared blank even though it was assigned to a partner administrator. (BBGRD-4601)

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

Threat or vulnerability	Description
Updated rule for advanced detection of using BCDEdit with the safeboot argument	• **Rule Name**: "Bcdedit Safeboot Modified" • **MITRE Techniques**: T1562, T1562.009 • **Description**: This detection rule identifies instances where the bcdedit command is executed with the safeboot argument. BCDEdit is a command-line tool used for managing Boot Configuration Data (BCD). Attackers may use the safeboot argument to reboot a system into Safe Mode to potentially disable security controls such as antivirus or endpoint detection tools, which might not operate in Safe Mode. • **Rule Type**: Advanced Detection • **Platform**: Windows • **Additional Reference**: MITRE • **Date added**: March 2025
Updated rule for advanced detection of the dsquery command	• **Rule Name**: "Dsquery Command Execution" • **MITRE Techniques**: T1087, T1087.002, T1482, T1082, T1018 • **Description**: This rule detects usage of the dsquery command. This command line utility can be used to query Active Directory (AD) from the host. • **Rule Type**: Advanced Detection • **Platform**: Windows • **Additional Reference**: MITRE • **Date added**: March 2025
Updated rule for advanced detection of suspicious process launches involving cryptographic operations	• **Rule Name**: "Suspicious Cryptographic Activity" • **MITRE Techniques**: T1027, T1055, T1486, T1573, T1573.001 • **Description**: This rule detects suspicious process launches involving cryptographic operations, such as AES, commonly abused by SolarMarker and Luma malware. • **Rule Type**: Advanced Detection • **Platform**: Windows • **Additional Reference**: Squiblydoo • **Date added**: March 2025

Threat or vulnerability	Description
Updated rule for advanced detection of the execution of gsecdump for credential dumping	• **Rule Name**: "Credential Dumping via gsecdump" • **MITRE Techniques**: T1003, T1003.001, T1003.002, T1003.004 • **Description**: This rule detects the execution of gsecdump, a tool used for credential dumping on Windows systems. Credential dumping involves extracting password hashes, plaintext passwords, or other authentication tokens from the operating system. The execution of gsecdump can target various credential storage locations including the Local Security Authority Subsystem Service (LSASS) and the Security Accounts Manager (SAM) database. False positives are less likely with this rule. • **Rule Type**: Advanced Detection • **Platform**: Windows • **Additional Reference**: MITRE and Red Canary • **Date added**: February 2025
Updated rule for advanced detection of a base64-encoded Bitstransfer download using PowerShell	• **Rule Name**: "Base64 Encoded PowerShell Execution of Bitstransfer" • **MITRE Techniques**: T1059, T1059.001, T1105, T1071, T1197 • **Description**: This rule detects the execution of a base64 encoded Bitstransfer download via PowerShell. Adversaries will obfuscate PowerShell Bitstransfer download commands to download malicious payloads and evade detection. False positives though unlikely can be occur from legitimate system admin tools and scripts. • **Rule Type**: Advanced Detection • **Platform**: Windows • **Additional Reference**: Medium • **Date added**: February 2025
Updated rule for advanced detection of a base64-encoded invocation of the System.Net.Webclient class using PowerShell	• **Rule Name**: "Base64 Encoded PowerShell Execution of .NET Webclient" • **MITRE Techniques**: T1059, T1059.001, T1105, T1071 • **Description**: This rule detects the use of a base64 encoded invocation of the System.Net.Webclient class via PowerShell. Adversaries will use System.Net.Webclient to download malicious payloads. False positives, though unlikely, can occur from legitimate system admin tools and scripts. • **Rule Type**: Advanced Detection • **Platform**: Windows • **Additional Reference**: Medium • **Date added**: February 2025
Updated rule for advanced detection of a base64-encoded Invoke-Restmethod command using PowerShell	• **Rule Name**: "Base64 Encoded PowerShell Execution of Invoke-Restmethod" • **MITRE Techniques**: T1059, T1059.001, T1105, T1071 • **Description**: This rule detects the execution of a base64 encoded Invoke-Restmethod command via PowerShell. Adversaries will use Invoke-Restmethod to download malicious payloads. False positives though unlikely can occur from legitimate system admin tools and scripts. • **Rule Type**: Advanced Detection • **Platform**: Windows • **Additional Reference**: Medium • **Date added**: February 2025

Threat or vulnerability	Description
Updated rule for advanced detection of a base64-encoded Invoke-Webrequest command using PowerShell	• **Rule Name**: "Base64 Encoded PowerShell Execution of Invoke-Webrequest" • **MITRE Techniques**: T1059, T1059.001, T1105, T1071 • **Description**: This rule detects the execution of a base64 encoded Invoke-Webrequest command via PowerShell. Adversaries will use Invoke-Webrequest to download malicious payloads. False positives though unlikely can occur from legitimate system admin tools and scripts. • **Rule Type**: Advanced Detection • **Platform**: Windows • **Additional Reference**: Medium • **Date added**: February 2025
Updated rule for advanced detection of comprehensive UAC bypass	• **Rule Name**: "Comprehensive UAC Bypass Detection" • **MITRE Techniques**: T1548, T1548.002, T1112, T1059, T1059.001 • **Description**: This rule detects UAC bypass attempts through registry modifications and PowerShell commands. It combines monitoring for specific registry keys, DelegateExecute, and PowerShell-based manipulations. • **Rule Type**: Advanced Detection • **Platform**: Windows • **Additional References**: Splunk and Sevagas • **Date added**: January 2025
Updated rule for advanced detection of AMSI bypass using PowerShell Command Execution	• **Rule Name**: "AMSI Bypass PowerShell Command Execution" • **MITRE Techniques**: T1059, T1059.001, T1562, T1562.001 • **Description**: This rule detects AMSI bypass through PowerShell by setting amsiInitFailed to true or by removing the registry key in HKLM\Software \Microsoft\AMSI. The Windows Anti-malware Scan Interface (AMSI) is a versatile interface standard that allows applications and services to integrate with any anti-malware product that's present on a device. AMSI provides enhanced malware protection for your end-users and their data, applications, and workloads. Adversaries disable AMSI to avoid possible detection of their malware, tools, and activities. False positives are not likely. • **Rule Type**: Advanced Detection • **Platform**: Windows • **Additional Reference**: Red Canary (AMSI InitFailed) and Red Canary (Remove AMSI Provider Reg Key) • **Date added**: January 2025

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 advanced detection of Windows Defender exclusion added via PowerShell	• **Rule Name**: "Windows Defender Exclusion Added via Powershell" • **MITRE Techniques**: T1562, T1562.001, T1059.001, T1059 • **Description**: This rule detects files or folder exclusions added to Windows Defender settings that may be an attempt to tamper with Windows Defender to possibly hide activity or evade detection. • **Platform**: Windows • **Additional reference**: Medium • **Date added**: November 2024
Updated rule for advanced detection of Standard RDP Port Modified	• **Rule Name**: “Standard RDP Port Modified” • **MITRE Techniques**: T1021, T1021.001, T1571 • **Description**: This rule detects the usage of RDP service and port modification. Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. This can be used by attackers to perform actions as logged on users. • **Platform**: Windows • **Additional reference**: MITRE • **Date added**: August 2024
Updated rule for advanced detection of GUARD: 8-character temp file created by Svchost	• **Rule Name**: “GUARD: 8 Character Temp File Created by Svchost” • **MITRE Techniques**: T1003, T1003.002 • **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**: Red Canary • **Date added**: August 2024
Updated rule for advanced detection of CylancePROTECT suspicious exit	• **Rule Name**: “CylancePROTECT Suspicious Exit” • **MITRE Techniques**: T1562, T1562.001, T1489 • **Description**: This rule detects suspicious exit events associated with the cylancesvc.exe process. CylancePROTECT has probably exited with an unexpected error code. Adversaries may disable or terminate security tools to interfere with security tools scanning and detection of their malware/tools and activities. • **Platform**: Windows • **Date added**: August 2024
Updated rule for advanced detection of CylancePROTECT suspicious exit via taskkill.exe	• **Rule Name**: “CylancePROTECT Suspicious Exit via taskkill.exe” • **MITRE Techniques**: T1562, T1562.001, T1489 • **Description**: This rule detects suspicious exit events associated with the cylancesvc.exe process via the execution of taskkill.exe. Adversaries may disable or terminate security tools to interfere with security tools scanning and detection of their malware/tools and activities. • **Platform**: Windows • **Date added**: August 2024

Threat or vulnerability	Description
Updated rule for advanced detection of Powershell scheduled task creation via Windows Script Host	• **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	• **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	• **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
Updated rule for advanced detection of the Csvde.exe export command	• **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

Threat or vulnerability	Description
Updated rule for advanced detection of local credential dump from NTDS, SAM or LSA using SecretsDump	• **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\Ntds.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	• **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
Updated rule for enhanced investigation of system information discovery through service enumeration	• **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

Threat or vulnerability	Description
Updated rule for advanced detection of the extraction of the domain database (including password hashes) using ntdsutil.exe	• **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	• **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	• **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
Updated rule for enhanced investigation of account or group discovery via dscl	• **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

Threat or vulnerability	Description
Updated rule for enhanced investigation of file and directory discovery through the Windows command line	• **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	• **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	• **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)
Updated rule for advanced detection of payload execution from Appdata\Local\Temp Directory	• **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

Threat or vulnerability	Description
Updated rule for advanced detection of Windows Defender service shutdown via net.exe	• **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
Updated rule for advanced detection of port forwarding SSH tunnel command execution	• **Rule Name**: "Port Forwarding SSH Tunnel Command Execution" • **MITRE Technique**: T1572, T1021, T1021.004 • **Description**: This rule detects when SSH is executed using the *-N* and *-R* 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
Updated rule for advanced detection of Windows Defender Antivirus Engine restored to default settings	• **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
Updated rule for advanced detection of obfuscated Bash History deletion	• **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

Threat or vulnerability	Description
Updated rule for advanced detection of Bash History modification and deletion	• **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	• **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	• **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 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
Updated rule for advanced detection of Svchost launching Rundll32 via scheduled task	• **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

Threat or vulnerability	Description
Updated rule for advanced detection of debugger registry value modification for accessibility features	• **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
Updated rule for advanced detection of obfuscated Base64 decoding method executed via PowerShell	• **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
Updated rule for advanced detection of UAC Bypass via fodhelper.exe activity	• **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

Threat or vulnerability	Description
Updated rule for advanced detection of payload creation via compiled HTML (CHM) file	• **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

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