Endpoint Privilege Management for Windows 24.1.108 Release Notes

March 26, 2024

Requirements:

- Microsoft .NET Framework 4.6.2 (required to use Power Rules, PowerShell audit scripts, PowerShell API, and Agent Protection)
- Microsoft .NET Framework 4.8 (required to use Multifactor Authentication with an OIDC provider)
- PowerShell 3.0 (required to use Power Rules, PowerShell audit scripts, and PowerShell API)
- Trellix (formerly McAfee) Agent (required if you are installing the Privilege Management client with switch **EPOMODE=1**)

> ***Note:*** *The executable version of the client package includes all necessary prerequisites (excluding .NET Framework) and automatically installs them as necessary. If you use the MSI or ZIP package, you must manually install any necessary prerequisites.*

New Features and Enhancements:

- Updated the MMC UI to change Azure AD references to Microsoft Entra ID.

Issues Resolved:

- Resolved an issue where the Defendpoint service would become unresponsive due to slow BeyondInsight server communication.
- Resolved an issue where copying content items in MMC Policy Editor would not copy controlling process groups.
- Resolved an issue where some **EXE** files started from the **Run as Administrator** context menu, which were not matched in policy rules and required UAC, would not start.
- Resolved an issue with updating group policy with EPM-W 23.9 and later.
- Added a **Desktop** and **Start Menu** shortcut for the Challenge Response Generator.
- Resolved an issue with *No License* events processing when EPM-W wasn't being used.
- Resolved an issue with Content Rules not correctly applying when using Notepad++ (version 8.4 and later) as the editor.
- Resolved an issue where copying applications in MMC wasn't copying dependent groups (e.g. child inheritance and parent groups).

Security Updates:

- Updated the QuickStart for Windows policy templates for Process Explorer to prevent malicious use against BeyondTrust Endpoint Privilege Management for Windows. We recommend updating your QuickStart based policies following this KB: https://beyondtrustcorp.service-now.com/csm?id=kb_article_view&sysparm_article=KB0020784.
- Resolved issues with the QuickStart policy for Mac. An attacker could bypass anti-tamper protection using AppleScript to call the **pmfm** utility as an elevated user.
- Updated the QuickStart for Windows templates to block Process Hacker to prevent malicious use against BeyondTrust Endpoint Privilege Management for Windows. We recommend updating your QuickStart based policies following this KB: https://beyondtrustcorp.service-now.com/csm?id=kb_article_view&sysparm_article=KB0020927.

- Resolved an issue with **.reg** files in a block rule. The block rule was bypassed when running the **.reg** file using **reg.exe**.
- Resolved an issue with the QuickStart for Windows and Discovery policy templates. An incorrectly defined application definition could permit the launch of some restricted applications without the appropriate message or auditing. We recommend updating your QuickStart based policies following this KB: https://beyondtrustcorp.service-now.com/csm?id=kb_article_view&sysparm_article=KB0020928.
- Resolved an issue with default policy rules in the QuickStart policy for Mac. Default policy rules blocking certain commands could be bypassed, allowing standard users to gain access to an interactive root shell or modify group membership to evade protection entirely.

Compatibility:

- Endpoint Privilege Management Policy Editor **24.1 (recommended)**, 22.1+
- Endpoint Privilege Management ePO Extension **23.10 (recommended)**, 22.7+
    - ePO Extension 23.10 requires BeyondTrust Privilege Management App (ePO) 24.1+
- Endpoint Privilege Management Console Windows Adapter **24.1 (recommended)**, 22.1+
- BeyondInsight/Password Safe **23.3 (recommended)**, 7.2+
- Trellix Agent **5.7+**
- Trellix ePO Server **5.10 Service Pack 1 Update 1(recommended)**, Update 13+
    - For 5.10 SP1 Update 2 see the KB article: BeyondTrust Compatibility with Trellix ePO

Supported Platforms:

For more information, see Endpoint Privilege Management for Windows Supported Platforms.

Notes:

None.