Xerox Security Bulletin XRX19-028

Xerox® EFI® Print Servers

For: Windows Operating System
Install Method: Update Manager

Deliverable: Microsoft OS Patches for Windows 7, 8.1, and 10
Includes: Windows patches
Bulletin Date: October 29, 2019

1.0 Background

Microsoft® delivers Critical Patch Updates (CPU) to address US-CERT-announced Security vulnerabilities and deliver reliability improvements to the Windows Operating platform. Microsoft® provides these patches to the public and authorizes vendors like Xerox® to deliver them to Customers with active Fiery® Print Server Support Contracts (FSMA).

This bulletin announces the availability of the following:

Variant	Description	CVE	Codename	More info
Initial	Intel Microarchitectural Data Sampling CPU Vulnerability	CVE-2018 12126 CVE-2018-12127 CVE-2018-12130 CVE-2019-11091	Zombieload	Intel Website Microsoft Website

Note: Xerox recommends that customers evaluate their security needs periodically and if they need Security patches to address the above CVE issues, should download all applicable fixes from Microsoft via Windows Update Manager.

2.0 Applicability

The following Microsoft Operating System updates are available.

1. Fiery servers running Windows 10 Operating System.

   - Microsoft has released a Windows update on May 14, 2019. Applying the Windows update will protect the systems against this vulnerability.
   - Microsoft has made this update available through their Microsoft Update Catalog, at: https://www.catalog.update.microsoft.com/search.aspx?q=4091664
   - The specific version that applies to Fiery servers is “2018-10 Update for Windows 10 Version 1607 for x64-based Systems (KB4091664)”.

2. Fiery servers running Windows 7 or 8.1 Operating System.

   Microsoft has not released an OS update to protect against this vulnerability. Microsoft has not released a schedule by when the updates will be available.

3.0 Windows 7 and 8.1 Mitigations

To protect your system from these vulnerabilities, Microsoft recommends that you take the following actions, and refer to the subsequent sections for links to further information for your specific situation:

1. The best protection is to keep computers up to date. This includes installing OS and microcode updates.

   - To be fully protected, customers may also need to disable Hyper-Threading (also known as Simultaneous Multi Threading (SMT)). Please see Knowledge Base Article 4073757 for guidance on protecting Windows devices.
   - OEMs might also provide additional guidance. Please visit the EFI Sales Portal for more detailed information. Access to this documentation requires a Sales Portal Account Registration.

2. Microsoft recommends that enterprise customers review this advisory in detail and register for the security notifications mailer to be alerted of content changes to this advisory. See Microsoft Technical Security Notifications.

3. Software developers should review the C++ developer guidance for speculative execution side channels.

4. Verify the status of protections for the various CVEs by running the PowerShell script Get-SpeculationControlSettings. For more information and to obtain the PowerShell script see Understanding Get-SpeculationControlSettings PowerShell script output.

4.0 Installation

Installation instructions will be included in the release notes with the Microsoft updates.