White Paper
May 2022

Microsoft Updates on DeltaV™ Systems

Introduction

The DeltaV™ automation system is supplied as a system with published performance specifications and customer expectations for robustness, integrity, and system responsiveness in line with the critical nature of automation systems. Emerson meets these automation system performance expectations by designing, and rigorously testing, DeltaV software with specific, known sets of Microsoft Windows® operating system versions and configurations.

Specific Concern for this Guideline[1]

Emerson recognizes that our customers are concerned with staying current with Microsoft security updates, critical updates, and service packs while still maintaining a supported DeltaV digital automation system configuration.

This document defines Emerson's guidelines around the testing and deployment of security updates, operating system updates and new operating system service packs.

Guideline

Emerson is concerned with maintaining the ongoing security and integrity of the operating system used on the DeltaV system. Therefore, all published Microsoft security updates and critical operating system updates are reviewed to determine whether deployment is permitted on the DeltaV automation system.

Emerson only supports updates that have been certified by Emerson for use with the applicable version of DeltaV system.

Microsoft Security Updates – Microsoft issues new security updates each month.

- From Windows 10 and Server 2016, Microsoft updates are now cumulative. Each cumulative update rolls new and previous (product and security) updates into one. There is no option to select 'Security Only Updates.'
- Each update published in Microsoft Security Bulletins is reviewed by Emerson for applicability to the DeltaV workstations the day Microsoft publishes the associated Security Bulletin.
- The result of Emerson's review is published in a Knowledge Base Article (KBA).
- This KBA indicates whether the security update or other directions contained in the security bulletin will be supported on the DeltaV system, and the estimated time until compatibility certification testing will be completed.

[1] *Guideline papers are issued to provide information concerning the practices that should be used for installation and deployment of a DeltaV system that is to be supported by Emerson. It is important that these guidelines be followed in order for Emerson to provide technical support for your DeltaV system. Failure to follow these guidelines may compromise our ability to provide timely and complete technical support for your DeltaV digital automation system.*

- Security updates are tested on the DeltaV system per an update-specific test plan.
- Implementation instructions for each security update on the DeltaV system is documented in the KBA.
- Security updates will be approved only in situations where they apply to an operating system feature/capability that is supported on the DeltaV system.
- Emerson tests security updates simultaneously across all supported versions of DeltaV software.
- Our goal is to complete security update certification testing for all supported DeltaV versions in 7 days.
- In some cases, a security update will be of sufficient complexity that evaluation and testing will require more effort and investigation than normal. In these relatively infrequent cases, certification and testing may fall outside the 7-day goal. In any case, Emerson works to get security updates tested and certified as quickly as possible.
- If testing reveals problems that require changes to DeltaV software for the security update to be installed, this information will be published with an explanation of how and when the issue will be resolved.
- Should Microsoft cease supplying security updates for any operating system version used to run DeltaV software, Emerson will stop supporting security bulletins for the DeltaV systems using that operating system.

Microsoft Critical Updates – Microsoft publishes critical updates (i.e., operating system defect repairs that do not pertain to security) whenever such a need arises.

- All Microsoft published critical updates are reviewed by Emerson.
- Unless the update is to be deployed on the DeltaV system, the results of this review are not published.
- Generally, updates that are not published by Emerson do not affect proper operation of DeltaV systems and their deployment is not supported.
- If a critical update is to be deployed on the DeltaV system, it will be documented in a KBA and follow the same procedure defined for security updates.

Deployment of Security Updates onto DeltaV Workstations

The nature of a control system, where operators are engaged in critical operations, requires that maintenance of the system be done with the knowledge and permission of the operators and operations staff.

Many security updates require a computer reboot to complete and should only be done within a maintenance window with operator knowledge and agreement. If a DeltaV workstation must be rebooted, the computer must come back online quickly to minimize disruption. The deployment of updates should not be configured to “install on next reboot,” as this would delay the reboot.

Taking control of a workstation with administrative software or by a remote administrator (except when requested and with the permission of operations) must be avoided.

Acquisition and Deployment Methods

Guardian subscribers can acquire certified update files and associated KBAs for download directly from the Emerson support website. Non-service subscribers should contact their local Emerson service office or business partner to request KBAs and update files. Depending on service agreement level and system version, a service can be set up to automatically deliver system-specific updates to an internet-facing non-DeltaV computer (typically the system control engineer's office PC) via the internet.

Distribution of update files to each DeltaV system workstation and server is accomplished either through the Integrated Patch Management for DeltaV service, or Guardian subscribers can download them manually. If manually patching, care must be taken to ensure the distribution media (USB flash drive for example) is free of malware.

Summary

The DeltaV operating system management guidelines simplify the administration of your system. Reviewing and testing only the system updates that impact DeltaV applications ensures that there are a very limited number of updates to install. We eliminate the guesswork of figuring out which patches to deploy. Emerson's Integrated Patch Management (IPM) is part of a security strategy that automates update deployment routines. IPM is easy, cybersecure by design and built for DeltaV.

The Emerson logo is a trademark and service mark of Emerson Electric Co. All other marks are the property of their respective owners.

The contents of this publication are presented for informational purposes only, and while diligent efforts were made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the designs or specifications of our products at any time without notice.

Contact Us
www.emerson.com/contactus

©2022, Emerson. All rights reserved.