AgriLife WSUS Report Status Message Definitions

Security Bulletin

The Security_Bulletin column indicates the year and sequence an update was released. MS13-047 is one of the most recent updates released. The 13 indicates this patch was released in 2013 and the 47 indicates the sequence number of the patch. For a precise release month and day Google 'MS13-047 release date'. The results of the search will show a release date of June 11, 2013. Review of the reports shows a few units with patches dating back a few years. If this applies to one of your systems please make every effort to resolve those patch updates first and then move on to the more recent ones.

Status

The Status column provides an indicator of the progress made for a released patch. There are four different indicators used: Not Installed, Downloaded, Installed Pending Reboot and Failed. A brief description of what each means is provided below.

Status = Not Installed

Not Installed means the update is not yet installed – there is no one reason the attempt has not been made but could include any of the following: installation attempt had not been made at the time of report generation, installation process was denied by end user, the download source was not accessible during the most recent attempt to install the update

Status = Downloaded

Downloaded indicates the update has been downloaded and is sitting on the system waiting to be installed.

Status = Installed Pending Reboot

Installed Pending Reboot indicates the update has been downloaded, installed, and is marked as requiring a reboot.

Status = Failed

Failed indicates the update was downloaded, an attempt was made to install the update and that attempt failed

Severity Rating

The Severity_Rating column utilizes five primary indicators to differentiate the impact of vulnerabilities: Critical, Important, Moderate, Low and Unspecified. Microsoft devised these indicators plus definitions to help decide which updates should be applied under particular circumstances and how rapidly those updates should be applied. A copy of the ratings indicators, their definition and Microsoft's recommended response time is provided below.

Rating - Critical

Definition - A vulnerability whose exploitation could allow code execution without user interaction. These scenarios include self-propagating malware (e.g. network worms), or unavoidable common use

scenarios where code execution occurs without warnings or prompts. This could mean browsing to a web page or opening email.

Microsoft recommends that customers apply Critical updates immediately.

Rating - Important
Definition - A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources. These scenarios include common use scenarios where client is compromised with warnings or prompts regardless of the prompt's provenance, quality, or usability. Sequences of user actions that do not generate prompts or warnings are also covered.

Microsoft recommends that customers apply Important updates at the earliest opportunity.

Rating - Moderate
Definition - Impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations.

Rating - Low
Definition - Impact of the vulnerability is comprehensively mitigated by the characteristics of the affected component.

Rating – Unspecified
Definition – The update does not have a severity rating.