



Wyse Security Bulletin WSB09-01 – Important

Security Update available for Wyse Device Manager

Release date: July 10, 2009
Update date: September 14, 2009
Version: 3.0

Platforms: WDM Server 4.7.x, Wyse thin clients running XPe, WES, Wyse Linux, CE6

Summary:

Buffer overflow vulnerabilities have been reported in WDM Server and the WDM HAgent. A carefully crafted packet sent to the WDM Server port, WDM tftp port, or the WDM Agent would crash the service, and could potentially allow the attacker to take control of the affected system. The security update addresses the vulnerability by modifying the way WDM validates the data and handles the error resulting in the exploitable condition.

Recommendation:

1. Wyse recommends that customers upgrade to the latest version of WDM (4.7.2) and apply the latest hotfix (HF 04072025609) at the earliest opportunity.
2. In addition, customers should deploy the new WDM HAgent included in the security update.
3. Customers using WDM Enterprise should configure HTTPS as the communication protocol.

The security update can be downloaded from:

Wyse.com | Support | Software Downloads - select Wyse Device Manager and click Search

Support:

<http://www.wyse.com/serviceandsupport/contact.asp>

Acknowledgements:

Thanks to Kevin Finisterre for identifying the vulnerability.

Disclaimer:

The information provided in the Security Bulletin is provided "as is" without warranty of any kind. Wyse Technology disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Wyse Technology or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Wyse Technology or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.