

Exchange Server Rollup

First up this week: Microsoft just released Update Rollup 3 (UR3) for Exchange 2007 SP1. Update rollups collect hotfixes that have been issued since the last service pack or rollup. UR3 contains a number of interesting fixes, including a way to remove the "Sent by Microsoft Exchange 2007" tag line from delivery status notification messages. The complete list of fixes in UR3 is included in Microsoft Knowledge Base article 949870. There's also a new rollup, UR7, for sites using Exchange 2007 RTM; you can see its list of fixes in KB article 953469.

Next, a related news item. Some administrators reported problems starting Exchange 2007 SP1 services after the last rollup, UR2. This problem occurred because some Exchange services are written using managed code under the Microsoft .NET Framework. .NET applications can be digitally signed, which requires the framework to verify the signature when a binary is loaded and executed. As part of the signature check, the .NET loader tries to contact a Microsoft server that publishes the certificate revocation list (CRL) for Microsoft-issued certificates. If this connection request fails, the .NET loader decides that the CRL can't be loaded, but it takes such a long time to make this determination that the Service Control Manager (SCM) thinks startup failed for that service. Microsoft documented this behavior after UR2 in KB article 944752, but it's still not that well known, mostly because it affects only a small percentage of Exchange servers (those that can't directly connect to the Internet). Speaking of certificates, security, and the like: On July 8, Microsoft released its monthly set of security updates for Windows and related applications. This release is perfectly predictable, of course, because Microsoft long ago committed to a regular schedule of such releases. The unusual thing about this Patch Tuesday is that it includes an Exchange fix, as described in Microsoft Security Bulletin MS08-039; the bulletin describes two escalation of privilege vulnerabilities in OWA 2007 and OWA 2003. These vulnerabilities both require an attacker to trick a user into opening an email message containing malicious scripting code. The vulnerabilities are fixed by the latest rollups, UR3 and UR7, and by the updates available individually from the security bulletin