[MS-EVEN6]: EventLog Remoting Protocol Version 6.0

This topic lists the Errata found in the MS-EVEN6 document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

September 12, 2018 - Download

Errata below are for Protocol Document Version V23.0 – 2021/04/07.

Errata Published*	Description
2021/06/08	In Section 2.1.1, Server, updated authentication level description: Changed from: The EventLog Remoting Protocol Version 6.0 allows any user to establish a connection to the RPC server. The server uses the underlying RPC protocol to retrieve the identity of the caller that made the method call, as specified in the second bullet of section 3.3.3.4.3 of [MS-RPCE]. The server SHOULD use this identity to perform method-specific access checks, as specified in section 3.1.4. Changed to: The EventLog Remoting Protocol Version 6.0 allows any user to establish a connection to the RPC server. The server uses the underlying RPC protocol to retrieve the identity of the caller that made the method call, as specified in the second bullet of section 3.3.3.4.3 of [MS-RPCE]. The server SHOULD use this identity to perform method-specific access checks, as specified in section 3.1.4. The server MAY require the client connection to specify an authentication level of at least packet-level authentication (0x4), as specified in [MS-RPCE] section 2.2.1.1.8. The server SHOULD require the connection to use the packet-privacy authentication level (0x6). <4> ... <4> Section 2.1.1: For more information about the significance of packet-level authentication, see Windows NTLM Elevation of Privilege Vulnerability security update June 2021 [MSFT-CVE-2021-31958]. Applies to all versions, client and server, beginning with Windows Vista operating system and Windows Server 2008 operating system. In Section 2.1.2, Client, updated authentication level description: Changed from: The client MUST use RPC over TCP/IP (that is, ncacn_ip_tcp), as specified in [MS-RPCE], as the RPC protocol sequence to communicate with the server. The higher-level protocol or client application MUST specify the Simple and Protected GSS-API Negotiation Mechanism

Errata Published*	Description
	[MS-SPNG] (0x9), NTLM [MS-NLMP] (0xA), or Kerberos [MS-KILE] (0x10) as the RPC authentication service, as specified in [MS-RPCE], and the protocol client MUST pass this choice unmodified to the RPC layer. Changed to: The client MUST use RPC over TCP/IP (that is, ncacn_ip_tcp), as specified in [MS-RPCE], as the RPC protocol sequence to communicate with the server. The higher-level protocol or client application MUST specify the Simple and Protected GSS-API Negotiation Mechanism [MS-SPNG] (0x9), NTLM [MS-NLMP] (0xA), or Kerberos [MS-KILE] (0x10) as the RPC authentication service, as specified in [MS-RPCE], and the protocol client MUST pass this choice unmodified to the RPC layer. The client MUST specify packet-level authentication (0x4) or higher, as specified in [MS-RPCE] section 2.2.1.1.8. <5> <5> Section 2.1.2: For more information about the significance of packet-level authentication, see Windows NTLM Elevation of Privilege Vulnerability security update June 2021 [MSFT-CVE-2021-31958]. Applies to all versions, client and server, beginning with Windows Vista and Windows Server 2008.

*Date format: YYYY/MM/DD