[MS-EVEN]: EventLog Remoting Protocol

This topic lists the Errata found in the MS-EVEN 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

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 server RPC interface is identified by UUID 82273FDC-E32A-18C3-3F78-827929DC23EA version 0.0, using the RPC well-known endpoint \PIPE\eventlog. The server MUST specify RPC over named pipes (that is, ncacn_np) as the RPC protocol sequence to the RPC implementation, as specified in [MS-RPCE]. The server MUST specify the Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) (0x9) or NT LAN Manager (NTLM) (0xA), or both, as the RPC Authentication Service (AS) (as specified in [MS-RPCE]). See [MS-RPCE] section 3.3.1.5.2.2 and [C706] section 13. Changed to: The server RPC interface is identified by UUID 82273FDC-E32A-18C3-3F78-827929DC23EA version 0.0, using the RPC well-known endpoint \PIPE\eventlog. The server MUST specify RPC over named pipes (that is, ncacn_np) as the RPC protocol sequence to the RPC implementation, as specified in [MS-RPCE]. The server MUST specify the Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) (0x9) or NT LAN Manager (NTLM) (0xA), or both, as the RPC Authentication Service (AS) (as specified in [MS-RPCE]). See [MS-RPCE] section 3.3.1.5.2.2 and [C706] section 13. The server MAY require the client connection to specify an authentication level of at least packet-level authentication (0x4), as specified in section 2.2.1.1.8 of [MS-RPCE]. The server SHOULD require the connection to use the packet-privacy authentication level (0x6).<5> ... <5> 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 named pipes (that is, ncacn_np), as specified in [MS-RPCE], as the RPC protocol sequence to communicate with the server. The client MUST specify either SPNEGO (0x9) or NTLM (0xA) (as specified in [MS-RPCE]) as the Authentication Service (AS).

Errata Published*	Description
	Changed to: The client MUST use RPC over named pipes (that is, ncacn_np), as specified in [MS-RPCE], as the RPC protocol sequence to communicate with the server. The client MUST specify either SPNEGO (0x9) or NTLM (0xA) (as specified in [MS-RPCE]) as the Authentication Service (AS). The client MUST specify packet-level authentication (0x4) or higher, as specified in [MS-RPCE] section 2.2.1.1.8.<6> ... <6> 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