Why do Hirschmann products still support the RC4 encryption algorithm?

- 2024-09-19 - Produkte

For users who cannot update their Windows XP and Windows 2003 servers Hirschmann products still offer RC4 support, thus these products can be managed securely. RC4 allows to disable HTTP ensuring that user credentials are never sent unencrypted over the network. After downloading the Java applet from the device the web interface establishes a dedicated HTTPS connection to the device using state of the art algorithms, and transmits the user credentials over this connection. Windows XP and Windows 2003 Server do not support more secure algorithms.
Users with newer operating systems can use better algorithms also available by Hirschmann products.

All known weaknesses in RC4 can only be exploited under special conditions that are not realistically applicable to embedded devices like Hirschmann network equipment. The most efficient attack requires that the web interface can be tricked to establish at least 16 million (2^24) connections with the same data. For technical details and risk assessment see http://www.isg.rhul.ac.uk/tls/#TLSsafe

With HiOS 6.0 and HiSecOS 4.0 TLS protocol versions and encryption algorithms can be configured to meet highest security requirements. If compatibility with older software like Windows XP, Windows 2003 Server, Java 6 and OpenSSL 0.9.8 is not required, TLS 1.0 and RC4 can be disabled.