Critical HMI Vulnerabilities – SPNEGO, SWEET32, NLA and RDP MiTM

Overview

GE Gas Power has been made aware of a set of vulnerabilities impacting Control Server Virtual HMIs and ThickClient HMIs across several versions of Windows Server. Please see below for further information on the individual vulnerabilities, affected products, and patching instructions.

Affected Products and Versions

Control Server Virtual HMIs and ThickClient HMIs, running the following Windows OS versions:

Windows Server 2012 R2
Windows Server 2016
Windows Server 2019

Vulnerability Details

1. SPNEGO

SPNEGO stands for Simple and Protected GSSAPI Negotiation Mechanism and is an internet standard for negotiating which Generic Security Service Application Program Interface (GSSAPI) technology is used for authentication between a client and server.

NEGOEX is an extended negotiation mechanism for SPNEGO (SPNEGO NEGOEX) intended to enhance SPNEGO by addressing some of the drawbacks of SPNEGO while adding new GSSAPI extensions.

Both Server Message Block (SMB) and Remote Desktop Protocol use NEGOEX for authentication by default, while Simple Mail Transfer Protocol (SMTP) and HTTP can be configured to do so. Please note that this is not an exhaustive list of protocols that use or can be configured to use SPNEGO NEGOEX.

CVE-2022-37958 is a remote code execution (RCE) vulnerability in the SPNEGO NEGOEX protocol of Windows operating systems, which supports authentication in applications.

CVE Details: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37958

2. SWEET32

SWEET32 is an encryption protocol used to provide secure connection in a client-server connection. This protocol uses the 3DES encryption suite, which causes the remote host supports the use of SSL ciphers that offer medium strength encryption. The SWEET32 attack is based on a security weakness in the block ciphers used in cryptographic protocols. It's similar to the RC4 attacks in terms of computational complexity.

In the Triple-DES and Blowfish algorithms, the block size is 64 bits, while for AES, they are 128. The shorter a block size is, the more vulnerable it is to a birthday attack — a type of vulnerability based on the birthday problem in probability theory. This makes 128-bit ciphers like AES more secure.

The DES and Triple-DES algorithms have been widely used to encrypt block ciphers for major protocols like TLS, SSH, and OpenVPN. This means a malicious user can obtain access to HTTP session cookies under the right conditions. The conditions include prolonged monitoring of traffic and executing JavaScript in the vulnerable browser that entails persuading a user to open an attacker-control website.

3. **NLA**

   NLA stands for Network Level Authentication. This particular authentication mechanism was not widely used in the past, as other authentication mechanisms did not have any major reported vulnerabilities or exploits. As cyber-criminals are becoming more motivated; these authentication protocols became less secure.

   If the remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

4. **RDP MiTM**

   Man-in-The-Middle (MiTM) attack is the nomenclature used for identifying attacks where an attacker intercepts a genuine and secure communication channel in-order to carry out Sniffing and/or Session Hijacking attack.

   When an RDP server issues a self-signed certificate, the certificate's authenticity cannot be verified by the connecting party, which can be exploited by attackers. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

   In our domain environment, RDP servers (VMs and ThickClients) can be configured to issues only CA cross-signed certificates using our Domain Enterprise CA. In a domain environment, authenticity of this certificate can easily be verified using thumbprint of the issuing CA server's certificate. Hence, it is essential that this feature is configured on all RDP servers on our controls network.

Exploitation Status

GE Gas Power Product Security is not aware of any malicious attempts to exploit these vulnerabilities in customer equipment.

Remediation

The patch for mitigation of SPNEGO vulnerability has been released as part of GE's September 2022 PPVP patches. The mitigation for SWEET32, NLA and RDP MiTM vulnerabilities have been addressed by GPO patches released by GE Gas Power. It is recommended that these patch implementations are carried out by qualified personnel.

Please contact your site CPM for further details on implementation of these patches.

Since the mitigation of these vulnerabilities is critical to maintain the plant network's security posture; please ensure these patches are implemented at the earliest available opportunity.

GE Power Product Security Incident Response Team (PSIRT)

Providing secure and reliable products and solutions is vital to the operations of GE Gas Power. Our products are engineered with security as a key principle. We have implemented and will maintain reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect our products and customers.

Contact Information

Contact your local GE Services representative for assistance or for additional information.
For Product Security issues or incident/vulnerability reporting: www.ge.com/power/cybersecurity

Document History

Version	Release Date	Purpose
1.0	June 5th, 2023	Initial release