

A part of **Department of Communications, Climate Action & Environment**



NCSC Advisory

CryptoAPI Spoofing Vulnerability – CVE-2020-0601
Windows RD Gateway and Windows Remote Desktop Client
Vulnerabilities – CVE-2020-0609, CVE-2020-0610, CVE-2020-0611

Status: **TLP-WHITE**

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

Traffic Light Protocol

This document is classified using Traffic Light Protocol. Recipients may share **TLP-WHITE** information freely, without restriction.

For more information on the Traffic Light Protocol, see http://en.wikipedia.org/wiki/Traffic_Light_Protocol

If you could treat this document according to the TLP assigned it would be greatly appreciated.

Technical Detail

1. Overview

Threat Type	Man-in-the-middle attacks Arbitrary Code Execution
Systems Affected	<p>CryptoAPI spoofing vulnerability – CVE-2020-0601: All machines running 32- or 64-bit Windows 10 operating systems, including Windows Server versions 2016 and 2019.</p> <p>Windows RD Gateway and Windows Remote Desktop Client Vulnerabilities – CVE-2020-0609, CVE-2020-0610, CVE-2020-0611: Windows Server 2012 and newer. In addition, CVE-2020-0611 affects Windows 7 and newer.</p>
Impact	<p>CryptoAPI spoofing vulnerability – CVE-2020-0601: A successful exploit could also allow the attacker to conduct man-in-the-middle attacks and decrypt confidential information on user connections to the affected software.</p> <p>Windows RD Gateway and Windows Remote Desktop Client vulnerabilities – CVE-2020-0609, CVE-2020-0610, and CVE-2020-0611: An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.</p>
Recommendations	Apply latest security updates from Microsoft.

2. Description

CryptoAPI spoofing vulnerability – CVE-2020-0601

A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates.

An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a ma-

licious executable, making it appear the file was from a trusted, legitimate source. The user would have no way of knowing the file was malicious, because the digital signature would appear to be from a trusted provider.

A successful exploit could also allow the attacker to conduct man-in-the-middle attacks and decrypt confidential information on user connections to the affected software.

Windows RD Gateway and Windows Remote Desktop Client vulnerabilities – CVE-2020-0609, CVE-2020-0610, CVE-2020-0611

CVE-2020-0609, CVE-2020-0610: A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction.

An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

CVE-2020-0611: A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server. An attacker who successfully exploited this vulnerability could execute arbitrary code on the computer of the connecting client. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would need to have control of a server and then convince a user to connect to it. An attacker would have no way of forcing a user to connect to the malicious server, they would need to trick the user into connecting via social engineering, DNS poisoning or using a Man in the Middle (MITM) technique. An attacker could also compromise a legitimate server, host malicious code on it, and wait for the user to connect.

3. Mitigation

Apply latest security updates from Microsoft.

Feedback and Reporting

NCSC-IE wishes to offer whatever assistance it can in relation to these vulnerabilities and is willing to work with the relevant parties to further understand the current threat. NCSC-IE would also request any feedback in relation to this incident as regards the relevance and accuracy of the information provided.