National Cyber Security Centre

2009170200-NCSC

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

NCSC Flash Alert

Critical Vulnerabilities in Microsoft Windows Netlogon Remote Protocol (MS-NRPC) CVE-2020-1472
2020-09-17

Status: TLP-WHITE

NCSC

Threat Type	The Microsoft Windows Netlogon Remote Protocol (MS-NRPC) reuses a known, static, zero-value initialization vector (IV) in AES-CFB8 mode. This allows an unauthenticated attacker to impersonate a domain-joined computer, including a domain controller and potentially obtain domain administrator privileges • CVE-2020-1472 - Netlogon Elevation of Privilege Vulnerability The vulnerability stems from a flaw in a cryptographic authentication scheme used by the Netlogon Remote Protocol, which among other things can be used to update computer passwords. This flaw allows attackers to impersonate any computer, including the domain controller itself, and execute remote procedure calls on their behalf.
Products Affected	Please see the Microsoft advisory for a full list of affected products: Microsoft Advisory
Impact	Unauthenticated Escalation of Privilege
Recommendations	NCSC-IE recommend that affected organisations apply the Microsoft patch issued in August 2020 on all Active Directory domain controllers as a matter of urgency. To address remaining risk, Windows will log warning events when certain legacy or third-party devices exist in the domain. In February 2021, enforcement mode, which will mandate Secure NRPC for all devices, will be turned on by default, requiring administrators to update, decommission or whitelist devices that do not support Secure NRPC beforehand. For further information please see the white paper by Secura.