Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Media release

UPDATE: ACSC confirms potential exploitation of BlueKeep vulnerability

12/08/2019

Thousands of Australian businesses using older Windows systems should immediately install a patch to avoid being compromised.

The Australian Signals Directorate (ASD) is aware of malicious activity that indicates potential widespread abuse of the BlueKeep vulnerability known as CVE-2019-0708, affecting older versions of Windows operating systems including the Windows Vista, Windows 7, Windows XP, Server 2003 and Server 2008 operating systems.

A security researcher under the Twitter handle *@zerosum0x0* has recently disclosed his Remote Desktop Protocol (RDP) exploit for the BlueKeep vulnerability to Metasploit. The disclosure, once made available to the public, is anticipated to increase the amount of RDP scanning actively, increasing the chances of attempted exploitation of unpatched systems.

The Head of ASD's Australian Cyber Security Centre (ACSC), Rachel Noble, estimated that up to 50,000 devices of Australian entities could be affected. "Any organisation or business that relies on the older Microsoft systems is at risk," Ms Noble said. "The compromise of an unpatched system could increase the chance that your network could be exploited."

The ACSC has already notified governments and critical infrastructure operators across Australia.

"ASD's ACSC is determined to ensure Australia is the safest place to connect online," Ms Noble said. "In simple terms, an unpatched system gives criminals a front door to break into your network and steal your corporate and customer information."

"Patching may require you to restart your computers but this is a small price to pay when the risk of a compromise occurring could harm your business and its customers."

The ACSC is acutely aware of the escalating scale and impact of cybercrime. Australian businesses need to be aware of the threat and we encourage them to follow our advice on how to strengthen their cyber defences and improve their resilience.

The threat is real but there is something you can do about it.

Protect your systems now

It is critical that organisations and individuals operating older versions of Windows systems **immediately install Windows' BlueKeep vulnerability patch - CVE-2019-0708**, available at www.microsoft.com/security/blog/2019/08/08/protect-against-bluekeep/

Windows users should deny access to Remote Desktop Protocols directly from the internet, or utilise a Virtual Private Network with multifactor authentication if Remote Desktop Protocols are required, regardless of the version of Windows you are running.

As a rule, it's important to always install manufacturers' updates as soon as possible.

On 6 June 2019 ASD provided advice on how to protect your systems against BlueKeep.