Microsoft Issues Emergency Security Updates for Windows 8.1 and Server 2012 R2

- Microsoft has issued an emergency out-of-band software update for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 systems to patch two new recently disclosed security vulnerabilities.

- Tracked as CVE-2020-1530 and CVE-2020-1537, both flaws reside in the Remote Access Service (RAS) in a way it manages memory and file operations and could let remote attackers gain elevated privileges after successful exploitation.

- In brief, the Remote Access Service functionality of the Windows operating system allows remote clients to connect to the server and access internal resources from anywhere via the Internet.

- On August 19, the company announced that Windows 8.1 and Windows Server 2012 R2 systems are vulnerable to both privilege escalation vulnerabilities and released out-of-band patches.

CVE-2020-1530 | Windows Remote Access Elevation of Privilege Vulnerability

- An elevation of privilege vulnerability exists when Windows Remote Access improperly handles memory.
- To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges.
- The security update addresses the vulnerability by correcting how Windows Remote Access handles memory.

CVE-2020-1537 | Windows Remote Access Elevation of Privilege Vulnerability

- An elevation of privilege vulnerability exists when the Windows Remote Access improperly handles file operations. An attacker who successfully exploited this vulnerability could gain elevated privileges.
- To exploit the vulnerability, an attacker would first need code execution on a victim system. An attacker could then run a specially crafted application.
- The security update addresses the vulnerability by ensuring the Windows Remote Access properly handles file operations.

It is highly recommended for Windows users and system admins to install newly available security patches as soon as possible to protect their servers against potential widespread attacks.

Source : Microsoft Security Response Center

Supported by : Ministry of Home Affairs (MHA), Govt. of India