COMPUTER SECURITY BULLETIN

Risk/Impact Rating: SERIOUS

< MS Windows LSASS DoS Vulnerability >

CSB17-005

Description:

Microsoft Windows LSASS is prone to a denial-of-service vulnerability. Successful exploitation of the issue will cause a denial of service on the target system's LSASS service, resulting in an automatic reboot of the system.

Technologies Affected

- Microsoft Windows 7 for 32-bit Systems SP1
- Microsoft Windows 7 for x64-based Systems SP1
- Microsoft Windows Server 2008 R2 for Itanium-based Systems SP1
- Microsoft Windows Server 2008 R2 for x64-based Systems SP1
- Microsoft Windows Server 2008 for 32-bit Systems SP2
- Microsoft Windows Server 2008 for Itanium-based Systems SP2
- Microsoft Windows Server 2008 for x64-based Systems SP2
- Microsoft Windows Vista Service Pack 2
- Microsoft Windows Vista x64 Edition Service Pack 2

Recommendations:

- Block external access at the network boundary, unless external parties require service;
- Run all software as a nonprivileged user with minimal access rights; and
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.

References:

https://www.symantec.com/security_response/vulnerability.jsp?bid=95318

http://www.securityfocus.com/bid/95318

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0004

https://www.checkpoint.com/defense/advisories/public/2017/cpai-2017-0010.html