SPACELABS HEALTHCARE

Security Advisory

Ref Doc ID	Version	Release Date	Advisory Status	Related CVE(s)
079-0286-00	A	2025-03-19	ACTIVE	CVE-2018-8693

1. VULNERABILITY INVESTIGATION

Spacelabs is aware of CVE-2018-8693 impacting Windows products. Spacelabs is investigating the impact of the vulnerability and/or known exploit which could affect Spacelabs products and will provide updates or response on this website: https://www.spacelabs.com/cybersecurity/advisories.

2. VULNERABILITY OVERVIEW

Spacelabs Healthcare has been made aware of an elevation of privilege vulnerability exists in Windows when Win32k component fails to properly handle objects in memory.

Supplier: Microsoft
Software name and version: Microsoft Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2009, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers
Software function and description: General Purpose Operating System
Affected versions: Microsoft Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2009, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers
Software use environment – Operating system

CVE-2018-8693

- **CVSS Score:** 7.8
- **CVSS Vector:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- **Attack Vector** – Win32k component
- **Attack Type** – Elevation of Privilege
- **Active Exploit** – Yes/No
- **CWE**-404 Improper Resource Shutdown or Release
- **Severity**: High

Potential Impact: The exploit allows the adversary to run arbitrary code in kernel mode then install programs; view, change, or delete data; or create new accounts with full user rights.

3. RISK ASSESSMENT SUMMARY

Spacelabs is in the process of assessing the potential impact of CVE-2018-8693 Win32k Component Failure vulnerability on our products. Once the assessment is complete, Spacelabs will provide follow-up notification with recommendations for corrective action.
As Spacelabs continue to gain a deeper understanding of the impact of this vulnerability, we will continue to publish technical information to help customers detect, investigate, and mitigate the vulnerability across all our products where applicable.

4. RECOMMENDATIONS

- Spacelabs recommends following up on this advisory. Notifications will be posted on the Spacelabs website https;//www.spacelabs.com/cybersecurity/advisories.
- Restrict network exposure for all Spacelabs products with the use of network segmentation, placement of these devices behind internal hospital firewalls, and ensure that they are not accessible from the Internet.

4.1 ASSESSMENT OF SPACELABS PRODUCTS

In response to the publication of this vulnerability, Spacelabs is conducting an assessment to identify devices potentially at risk of this vulnerability. Please note information is subject to change as the situation evolves.

SPACELABS HEALTHCARE

5. Additional Resources

#	RESOURCE	URL
1	CVE-2018-8693 Detail	https://www.cve.org/CVERecord?id=CVE-2018-8639
2	CISA Article	https://www.cisa.gov/news-events/alerts/2025/03/03/cisa-adds-five-known-exploited-vulnerabilities-catalog
3	NIST	https://nvd.nist.gov/vuln/detail/cve-2018-8639

6. Document History

Version	Release Date	Purpose
Rev A	2025-03-19	Microsoft Windows Win32k Component Failure Vulnerability Assessment and Potential Product Impact Statement.

7. Terms of Use

The information in this document is subject to change without notice. In no event will Spacelabs or any of its suppliers be liable for direct, indirect, special, incidental, or consequential damages of any nature or kind arising from the use of this document, even if Spacelabs or its suppliers have been advised of the possibility of such damages.

This document contains confidential and proprietary language and may not be reproduced or shared with a third party without written permission from Spacelabs. All rights to registrations and trademarks reside with their respective owners.