Olympus Response to Microsoft Remote Desktop Services Remote Execution Vulnerability (CVE-2019-0708)

Original Release Date: May 23, 2019 | Last Revised Date: May 23, 2019

Note: This communication is the result of initial and ongoing analysis and represents all actions taken by Olympus as of the last revised date. As a result, the content may change as information of the vulnerabilities are released, or additional actions are completed.

Olympus is aware of and currently monitoring ongoing developments related to the recent Microsoft critical vulnerability notification which could affect Remote Desktop Services.

Full information on the vulnerability can be found at the following Microsoft link:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

Olympus Actions & Mitigation Plan

Olympus consistently strives to enhance the security of our products. As such, a global team has been coordinated and is currently investigating which Olympus products may be affected by this vulnerability. Additionally, for any products that may be affected, Olympus will work to test the patches supplied by Microsoft and release once validated.

This page will be updated as new information becomes available.

More information and guidance from the United States Computer Emergency Readiness Team (US-CERT), as sponsored by the United States Department of Homeland Security (DHS), can be found at the link below.

https://ics-cert.us-cert.gov/Microsoft-Releases-Security-Update-Remote-Desktop-Services-Vulnerability