

IT



# SECURING THINGS

FOR SMART & SAFER SOCIETY

## Microsoft DCOM Vulnerability & Hardening Advisory (Risks, Mitigation & Preparation)

Author: M. Yousuf Faisal (Founder STL)

OT/IOT

# MS DCOM Vulnerability & Hardening Advisory – Risk, Mitigation & Preparation



**MS DCOM Hardening Brief**

DCOM Security Advisory Background and Timelines	14 <sup>th</sup> May 2023 - DCOM Hardening Windows Updates Applied by Microsoft. Disabling it, is no longer an option.	“Distributed Component Object Model” (DCOM) a technology used by Windows Applications to enable inter-process communication over a network.	Impacts = Both IT & OT/ICS Production Systems! Caution = Ensure Updates/Upgrades are planned.
---	--	---	--

**MS DCOM Hardening Patch – Risks & Impact Simplified**

MS - DCOM Vulnerability	June 8, 2021 - Microsoft revealed Windows DCOM Server Security Feature Bypass vulnerability - <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26414">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26414</a>	
MS – DCOM Patch (Fix)	Microsoft Fix called “DCOM Hardening” – Enforces DCOM Authentication on Server Side. Microsoft approach was a 3 phased roll-out. 14 <sup>th</sup> March 2023 was final phase. Post 14 <sup>th</sup> March 2023, disabling the hardening is no longer an option for an updated system. Doesn't impact local connections / MS Win XP systems / OPC UA.	
MS DCOM Hardening Explained	Microsoft DCOM hardening patch = prevents unauthorized access to computers via DCOM protocols, which may potentially lead to malicious attacks or data breaches. Once installed, this patch limits communications between different devices and applications; and may potentially cause disruptions to production systems.	
MS DCOM Usage	DCOM Remote Protocol is a protocol for exposing application objects using remote procedure calls (RPCs), used for comms b/w software components of network devices. Many Application software and automation instrument vendors have used DCOM to send / transfer data through the industrial network to HMIs, Historians, and the like.	
Impact on OT/IT Systems	Elevation of Privileges exploit   At Risk Win 7, 2008 SP2 or above, Non-Win DCOM clients/servers   All network devices under same security authority maybe exposed   unauthorized privilege access to modify settings, files, non-sensitive resources. May result in loss of integrity / protection of network devices & users files & settings.	
Recommendations	(a) Contact your IT/OT App Software vendor for a patch to mitigate any hardening disruption   (b) Upgrade from OPC-DA protocol to OPC-UA (UA don't use DCOM   (c) Install OPC Tunnellers (Converts protocol to more secure protocol to continue communications)   (d) use alternate controls like EDR Solution until upgrade/update.	
Reference / Example Guidance for Businesses from SIs / OEM Vendors	<ul style="list-style-type: none"> <li>• <a href="#">Siemens Guidance on MS DCOM Hardening</a></li> <li>• <a href="#">Siemens SIMATIC PCS7 Microsoft Update compatibility</a></li> <li>• <a href="#">Rockwell Automation Product Notification</a> (login required)</li> <li>• <a href="#">AVEVA DataHub Tunneller for OPC &amp; AVEVA Tech Alert</a></li> <li>• <a href="#">Yokogawa DCOM Hardening</a></li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">Microsoft DCOM hardening patch insights</a></li> <li>• <a href="#">KB5004442—Manage changes for Windows DCOM Server Security Feature Bypass (CVE-2021-26414)</a></li> <li>• <a href="#">OPC Data Client Apps &amp; DCOM Hardening (CVE-2021-26414, KB5004442)</a></li> <li>• <a href="#">DCOM Authentication Hardening: What you need to know</a></li> <li>• <a href="#">Microsoft Distributed Component Object Model (DCOM) Hardening Toolkit</a></li> </ul>

# DCOM Hardening Playbook Recommendations

**Intended Audience = IT Security and OT/ICS Security Team**

**Use Automated tools or Manual means to discover DCOM on the network**

Recommended Steps	Description of Activities
<b>1 – Discovery &amp; Inventory</b>	<ul style="list-style-type: none"><li>• Identify list of (existing in production) applications using DCOM functionality both in IT &amp; OT networks (e.g. OPC DA / Classic, and others) (also identify vendor and app version)</li><li>• Identify app owner and deployment type (central or by plant/site)</li></ul>
<b>2 – Remediation Preparation</b>	<ul style="list-style-type: none"><li>• Identify Impact for each app using DCOM</li><li>• Identify vendor support contracts, contact lists,</li><li>• Identify Remediation Plan (i.e., Upgrade, Patch, protocol change etc.) &amp; stakeholders (systems owner, vendor, implementor, tester etc.)</li><li>• Plan downtime and prepare documentation.</li></ul>
<b>3 – Test &amp; Assess</b>	<ul style="list-style-type: none"><li>• Review Event IDs (10036, 10037, 10038) for DCOM events</li><li>• Test on systems with latest patch and supported OS based on remediation plan and assess outcomes.</li></ul>
<b>4 – Implement Change (Install Patch / Upgrade / Change protocol)</b>	<ul style="list-style-type: none"><li>• Prioritize and roll-out phased implementation of changes to targeted systems specific to your environment (use maintenance windows to implement).</li></ul>
<b>5 – Verify &amp; Complete Remediation</b>	<ul style="list-style-type: none"><li>• Once implemented, verify the communications between network systems and complete the remediation tasks with any other application specific or OS specific patches to be applied.</li></ul>





# Securing Things Limited (STL) - Services Offerings (In Brief)

**Services Focus = IT & OT Cybersecurity & Technology Services & Solutions (Certain services spans across all 3 services pillars)**

## vCISO / Awareness Trainings



## IT Cybersecurity Services



## OT/ICS Cybersecurity Services



**vCISO & Awareness Training = IT & OT Cybersecurity Strategy/Program Development, awareness training, workshops, Partner On-Demand AppSec Training**

**GRC Advisory & Consulting = IT & OT Strategy/Policy development, Assessments/Discovery/Reviews/Audits/Gap Analysis for compliance e.g., IEC 62443, ISO 27001, PCI DSS, NIST CSF, CSC, other local/regional/global security standards & frameworks, STL OT Security Dozen and more) & Other customized services.**

**Threat & Vulnerability Management = Configuration Hardening Reviews, IT Vulnerability Scans (/OT passive discovery) and OSINT/Pen-testing (+via partners).**

**For Service Providers/Consulting Firms = Business Development (BDaaS) | Presales (PaaS) | Advisory/Consulting (ACaaS) Delivery - as a service model**

**Custom Project Needs = For Client/End user specific requirements & / combination of service offerings**

**IT Security Solutions = Select / Architect / Deploy / Review (Partner Solutions)**

**OT IDS/AD Solution = Select / Architect / Deploy / Review (Partner Solutions)**

**Delivery Model = Global / Remote (per time zone needs) – with occasional onsite visits/delivery where required.**

# Thanks

It's a great day to start ...



## For IT & OT Operations..

Contact: [info\[at\]securingthings\[dot\]com](mailto:info@securingthings.com)  
<https://securingthings.com>

*Note: Commercial Use or Re-Production of this copyright material is prohibited without permission of STL / Author.*

