



ROOT CAUSE ANALYSIS

Escalation Details					
Customer Name	Serco Sungard AS	Customer Designation	Head of ICT	Customer Email ID	peterg@ealing.gov.uk
Escalation ID	ML_ET_1000000667	Service Line	Wintel & Virtualisation	Client	Ealing
Escalation Category	Operational Process Failure	Ticket number	-NA-	Escalation Received Date	26/10/2023
RCA Assignment date	02/11/2023	RCA Completion Date	02/11/2023	RCA Approved Date	03/11/2023
RCA Assignment team	Wintel & Virtualisation	RCA Author(Esc Owner)	bradleyws	RCA Co-authors	PuttappaM; Baldeep Sood;Noushad Nazar;
Escalation Description	Ealing ICT Service Portal down due to disabling TLS 1.0				

Root Cause Details	
ROOT CAUSE	Corrective Action
Instead of applying the change CR1591646 to Disable SSL /TLS 1.0 &1.1 and Use TLS 1.2 (with approved cipher suites) or higher instead for only Test and Dev Servers the change was mistakenly applied to all the servers including production. The GPO created was applied to "Authenticated Users group" in the security Filtering. When Authenticated Users is present in the GPO Security Filtering, it implies that it can apply to any authenticated objects to which the GPO is linked (meaning any object/server present in the OU).	1) Removed Authenticated Users group from the security filtering and added Domain Computers Group in the delegation 2) Enabled TLS 1.0, TLS 1.1 and TLS 1.2 on all the affected SCSM and SCOM servers.



Preventive Action	Target Closure Date
1)Revisit the GPO changes and plan for proper implementation of the policy 2) Confirm with SCSM and SCOM vendor what TLS protocol the applications use and if disabling 1.0 and 1.1 will cause issues 3)Apply October Month patches to the SCSM and SCOM servers	06/11/2023

RCA Review Details			
Reviewer Name	NagarajaKG	Date Reviewed	03/11/2023
Approval Status	Approved	Reason for rejection (if rejected):	

Updates		
Date	Owner	Details