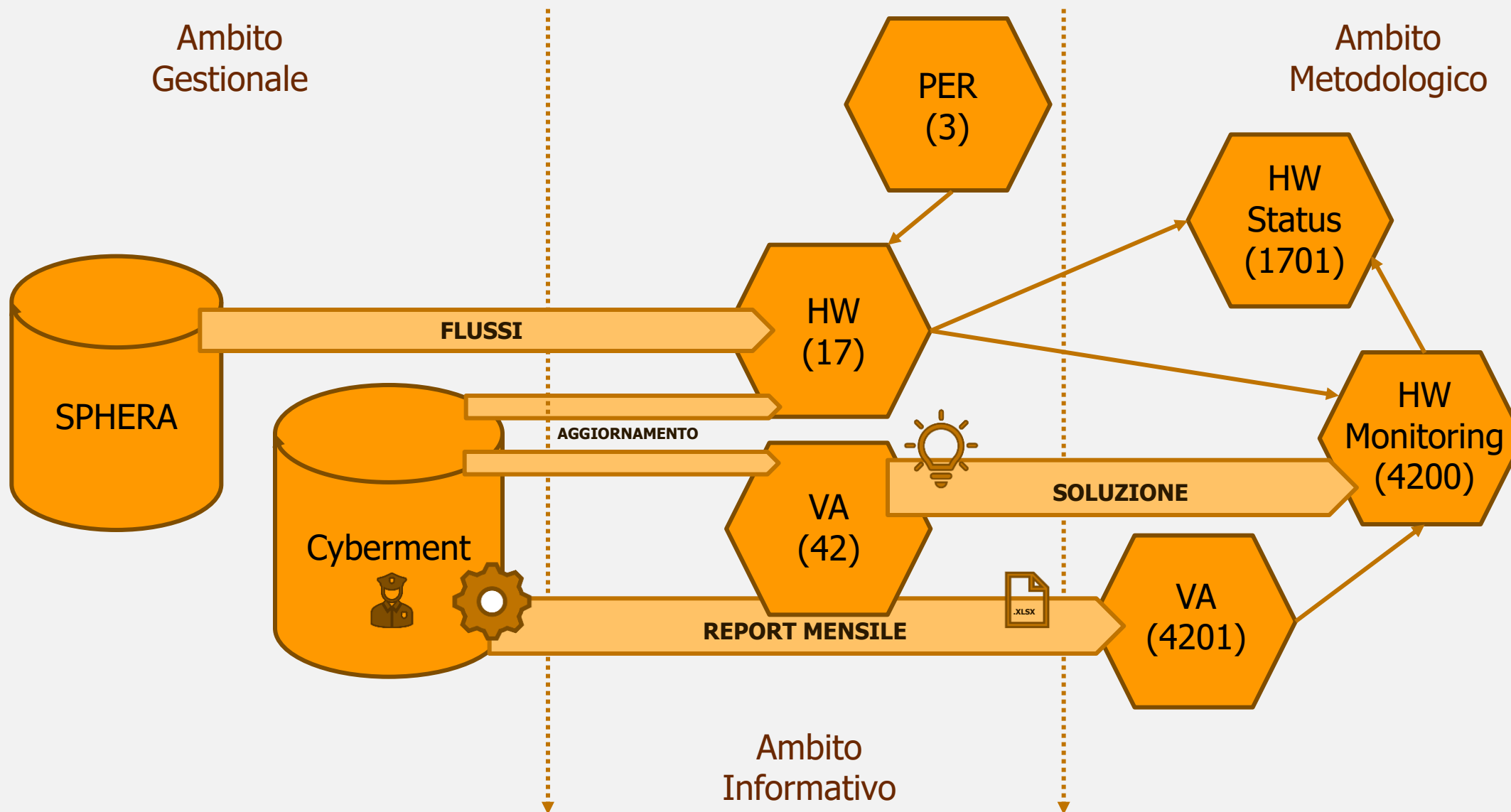




# **Automazione dei Controlli Vulnerability Assessment**



Scope: EQV - Assessment | Catalogue: HW - Management | Model type: HW - Management

Reference date: 10/07/2025 | Historic: OFF | Future: ON

Code	Acronym	Description	Assignee	Location	Supplier	Client	Economic	Strategic	Start	End
UPS	UPS	UPS					VH	HI	11/06/2018	
SRV	SRV	Server					VH	HI	11/06/2018	
SRV-EQV	SRV-EQV	HOST EQV (main)	TUB	SRV	EQV	EQV	VH	HI	11/05/2020	
SERVER-EQV	SERVER-EQV-60	SRVEQV 60 (DB)	TUB	SRV	EQV	EQV	MD	MD	14/06/2019	
SERVER-EQV	SERVER-EQV-200	SRVEQV 200 (Test)	TUB	SRV	EQV	EQV	MD	MD	14/06/2019	
SERVER-EQV	SERVER-EQV-10	SRVEQV 10 (Client)	TUB	SRV	EQV	EQV	VH	HI	14/06/2019	
PRI	PRI	Printer					NO	LW	11/06/2018	
PC	PC	Personal Computer					MD	MD	11/06/2018	
PC-TAT	PC-TAT	HP		HOM	EQV	EQV	NO	LW	01/08/2018	
PC-RAG-LOY	PC-RAG-LOY	PC-RAG-LOY	LOY	HOM	EQV		NO	LW	31/01/2025	
PC-OWN-ROG	PC-OWN-ROG	PC-OWN-ROG	ROG	HOM			NO	UN	01/06/2025	
PC-NON-ASS-2	PC-NON-ASS-2	PC-NON-ASS-2		PRJ.R2	EQV	EQV	NO	LW	29/01/2019	
PC-EQV-VEN	PC-EQV-VEN	PC-EQV-VEN	TAT	HOM	EQV	EQV	NO	MD	31/07/2018	
PC-EQV-TUB	PC-EQV-TUB	PC-EQV-TUB	TUB	HOM	EQV	EQV	NO	MD	12/06/2019	
PC-EQV-TAU	PC-EQV-TAU	PC-EQV-TAU	TAU	HOM	EQV	EQV	NO	HI	20/02/2020	
PC-EQV-TAT	PC-EQV-TAT	PC-EQV-TAT	TAT	HOM	EQV	EQV	NO	HI	09/05/2023	
PC-EQV-SAN	PC-EQV-SAN	PC-EQV-SAN	SAN	HOM	EQV	EQV	NO	HI	01/11/2018	

**CATEGORIZZAZIONE PER TIPOLOGIA HW**

**STATO DEL CATALOGO A DATA**

**PROPRIETÀ**  
Fruitore, Luogo, Fornitore e Cliente

Scope: EQV - Quality MS | Catalogue: VUL - Management | Model type: VA - Management

Drag a column header here to group by that column

Reference date: 10/07/2025 | Historic: OFF | Future: ON

Code	Acronym	Description	Severity	Exploit	Malware	Undeleteble	Action	Start	End	Order
383136	383136	Azure Data Studio Privilege Escalation Vulnerability	4.00					06/06/2025		0.00
383211	383211	VMware Tools Insecure File Handling Vulnerability (VMSA-2025-0007)	3.00					06/06/2025		0.00
110494	110494	Microsoft Office Security Update for May 2025	4.00					06/06/2025		0.00
92270	92270	Microsoft .NET Security Update for June 2025	4.00					09/07/2025		0.00
92212	92212	Microsoft PC Manager Elevation of Privilege Vulnerability for February 2025	4.00					09/07/2025		0.00
92255	92255	Microsoft PC Manager Elevation of Privilege Vulnerability for May 2025						09/07/2025		0.00

Page 1 of 7 (672 items) | 1 2 3 4 5 6 7

DESCRIZIONE VULNERABILITÀ

STATO DEL CATALOGO A DATA

GUIDA RISOLUTIVA

CODICI IDENTIFICATIVI

GRADO IMPATTO / RISCHIO

FLAG VULNERABILITÀ

383136 - Azure Data Studio Privilege Escalation Vulnerability - (EQV - Quality MS - VUL - Management)

**GENERAL DATA**

Code: 383136  
Acronym: 383136  
Description: Azure Data Studio Privilege Escalation Vulnerability  
Notes:  
Start date: Today 06/06/2025  
End date: Today  
QID: 383136

**VULNERABILITY DETAIL**

Severity: 4.00 (V4 - Very High)

Exploit:   
Malware:   
Brute force:   
Port: 0  
Protocol:  
SSL:  
Link: [Link Soluzione](#)  
Undeletable:

**ACTION**

andare qui: [Release February 2024 Release \(version 1.48.0\) - microsoft/azuredatastudio - GitHub](#)  
scaricare e installare questo:  
<https://github.com/microsoft/azuredatastudio/releases/tag/1.48.0>

New Item	Details
Installation	Azure Data Studio installation fails on RHEL 8 Use RHEL 9, or

For a list of the current known issues, visit the [issues list on GitHub](#).

Platform	Type	Download
Windows	User Installer	<a href="#">64 bit</a> <a href="#">ARM</a>
	System Installer	<a href="#">64 bit</a> <a href="#">ARM</a>
	.zip	<a href="#">64 bit</a> <a href="#">ARM</a>
Linux	.tar.gz	<a href="#">64 bit</a>
	.deb	<a href="#">64 bit</a>
Mac	.rpm	<a href="#">64 bit</a>
	zip	<a href="#">Universal</a> <a href="#">Intel Chip</a> <a href="#">Apple Silicon</a>

**CODICI IDENTIFICATIVI**

**DESCRIZIONE VULNERABILITÀ**

**GRADO IMPATTO / RISCHIO**

**FLAG VULNERABILITÀ**

**GUIDA RISOLUTIVA**

**CYBERMENT**

## Azure Data Studio Privilege Escalation Vulnerability

CYBID: 383136

Category: Local

CVE ID: CVE-2024-26203

Vendor reference: Security Update

Bugtraq ID:

Service Modified: 03/31/2020

User Modified:

Edited:

PCI Vuln: No

Ticked State:

**Threat:**  
Azure Data Studio is built on top of Visual Studio Code and offers a lightweight, keyboard focused modern code workflow experience when working with SQL Server, Azure SQL Database, and Azure Synapse Analytics. CVE-2024-26203: This is an elevation of privilege vulnerability affecting Azure Data Studio. An attacker who successfully exploits this flaw can gain elevated permissions within the application, potentially leading to unauthorized access or data manipulation.

**Affected Versions:**  
Prior to 1.48.0

**QID Detection Logic:(Authenticated):**  
This QID checks the vulnerable version of Azure Data Studio.

**Impact:**  
Successful exploitation allows an attacker to gain access to restricted files.

**Solution:**  
Customers are advised to refer to [Security Update](#) more details and patch information.  
Patch:  
Following are links for downloading patches to fix the vulnerabilities:  
[Security Update](#)

**Cyberment VUL DB**

Action

andare qui: [Release February 2024 Release \(version 1.48.0\) - microsoft/azuredatastudio - GitHub](#)  
scaricare e installare questo:  
<https://github.com/microsoft/azuredatastudio/releases/tag/1.48.0>

New Item	Details
Installation	Azure Data Studio installation fails on RHEL 8 Use RHEL 9, or

For a list of the current known issues, visit the [issues list on GitHub](#).

Platform	Type	Download
Windows	User Installer	<a href="#">64 bit</a> <a href="#">ARM</a>
	System Installer	<a href="#">64 bit</a> <a href="#">ARM</a>
	.zip	<a href="#">64 bit</a> <a href="#">ARM</a>
Linux	.tar.gz	<a href="#">64 bit</a>
	.deb	<a href="#">64 bit</a>
Mac	.rpm	<a href="#">64 bit</a>
	zip	<a href="#">Universal</a> <a href="#">Intel Chip</a> <a href="#">Apple Silicon</a>

Attività EQV - Assessment    Model HW - Vulnerability Assessme...    Analysis HW - Monitoring    Periodo 01/06/2025

**HW - Monitoring**

Drag a column header here to group by that column

**CONTROLLO PERIODICO**

Type	Code	Description	ECO	STR	P. Risk	R. Risk	Total	Susp	Undel	VH_Tc	LO_ToDo	ToBe	Exp/Mal	V5	V4	V3	V2	V1
Server	SERVER-EQV-10	SRVEQV 10 (Client)	VH	HI	VH	CO	8	0	0		0	0	1	0	2	0	5	0
Server	SERVER-EQV-60	SRVEQV 60 (DB)	MD	MD	HI	CO	3				0	0	0	0	1	0	2	0
Server	SRV-EQV	SRV EQV (main)	VH		LO	CO	5				0	0	0	0	0	0	5	0
Personal Computer	PC-EQV-DAN	PC-EQV-DAN	NO	MD	VH	CO	10				0	0	1	2	0	2	5	0
Personal Computer	PC-EQV-BEL	PC-EQV-BEL	MD	HI	ME	CO	2				0	0	0	0	0	1	1	0
Personal Computer	PC-EQV-TAT	PC-EQV-TAT	NO	HI	VH	LO	9				2	0	1	3	0	1	4	0
Personal Computer	PC-EQV-FIL	PC-EQV-FIL	NO	LW	VH	CO	4				0	0	1	0	0	0	3	0
Personal Computer	PC-EQV-TUB	PC-EQV-TUB	NO	MD	HI	CO	2				0	0	0	0	2	0	0	0
Personal Computer	PC-EQV-LUC	PC-EQV-LUC	NO	LW	ME	CO	1				0	0	0	0	0	1	0	0
Personal Computer	PC-EQV-ING	PC-EQV-ING	NO	HI	ME	CO	1				0	0	0	0	0	1	0	0
Personal Computer	PC-EQV-SAN	PC-EQV-SAN	NO	HI	VH	CO	2				0	0	0	1	0	1	0	0
Personal Computer	PC-EQV-CAR	PC-EQV-CAR	NO	HI	VH	CO	4	0	0		0	0	0	0	0	0	0	0
Personal Computer	PC-EQV-CAS	PC-EQV-CAS	NO	MD	VH	CO	8	0	0		0	0	0	0	0	0	0	0
DeskTop	DSK-EQV-SAN	DSK-EQV-SAN	LW	HI	VH	CO	10	0	0		0	0	0	0	0	0	0	0
Cloud Server	SERVER-EQV-SUR	HST-SUR (ARUBA)	LW	LW	HI	CO	9	0	0		0	0	0	0	0	0	0	0
Cloud Server	SERVER-EQV-BME	HST-BME (UNIDATA)	MD	MD	VH	CO	3	0	0		0	0	0	0	0	0	0	0
Cloud Server	SERVER-EQV-CDP	HST-CDP (ARUBA)	VH	HI	HI	CO	7	0	0		0	0	0	0	0	0	0	0
Cloud Server	CLOUD-EQV-BME	CLOUD-BME (Aruba)	NO	HI	HI	CO	3	0	0		0	0	0	0	0	0	0	0
Cloud Server	CLOUD-EQV-AMC	CLOUD-AMC (Aruba)	NO	HI	ME	CO	1	0	0		0	0	0	0	0	0	0	0

**Trend**

**Trend Line**

**RISCHIOSITÀ PRE e POST ATTIVITÀ**

**ATTIVITÀ DA ESEGUIRE (PER GRADO DI RISCHIO)**

Page 1 of 1 (19 items)

Attività EQV - Assessment    Model HW - Vulnerability Assesse...    Analysis HW - Status    Periodo 01/07/2025

**CONTROLLO PERIODICO**

HW - Status

Drag a column header here to group by that column

Type	Code	Description	ECO	STR	P. Risk	R. Risk	
(All)	Q	Q	(	(	(...	(All)	
Cloud Server	SERVER-EQV-AMC	<a href="#">HST-AMC (PORINI)</a>	VH	HI	LO	LO	
Cloud Server	SERVER-EQV-SUR	<a href="#">HST-SUR (ARUBA)</a>	LW	LW	VH	VH	
Cloud Server	SERVER-EQV-BME	<a href="#">HST-BME (UNIDATA)</a>	NO	UN	VH	VH	
Cloud Server	SERVER-EQV-CDP	<a href="#">HST-CDP (ARUBA)</a>	VH	HI	HI	HI	
Server	SERVER-EQV-10	<a href="#">SRVEQV_10 (Client)</a>	VH	HI	VH	VH	
Server	SERVER-EQV-60	<a href="#">SRVEQV_60 (DB)</a>	MD	MD	LO	LO	
Personal Computer	PC-EQV-BEL	<a href="#">PC-EQV-BEL</a>	MB	HI	VH	VH	
Personal Computer	PC-EQV-TAT	<a href="#">PC-EQV-TAT</a>	NO	HI	VH	VH	
Personal Computer	PC-EQV-DAN	<a href="#">PC-EQV-DAN</a>	NO	MD	VH	VH	
Personal Computer	PC-EQV-CAS	<a href="#">PC-EQV-CAS</a>	NO	MD	VH	VH	
Personal Computer	PC-EQV-CAR	<a href="#">PC-EQV-CAR</a>	NO	HI	VH	VH	
Personal Computer	PC-EQV-SAN	<a href="#">PC-EQV-SAN</a>	NO	HI	VH	VH	
<input checked="" type="checkbox"/>	Personal Computer	PC-EQV-LUC	<a href="#">PC-EQV-LUC</a>	NO	LW	HI	HI
Cloud Server	CLOUD-EQV-BME	<a href="#">CLOUD-BME (Aruba)</a>	NO	HI	HI	HI	

**RISCHIOSITÀ PRE e POST ATTIVITÀ**

**STORICO VULNERABILITÀ**

Trend

Trend Line

Severity

Page 1 of 7 (301 items)    Page 1 of 1 (14 items)



**CONTROLLO PERIODICO**

**RISCHIOSITÀ  
PRE e POST  
ATTIVITÀ**

**STORICO  
VULNERABILITÀ**

Attività: EQV - Assessment    Model: HW - Vulnerability Assessme...    Analysis: HW - VA ToDo    Periodo: 01/07/2025

**CONTROLLO PERIODICO**

HW - VA ToDo

HW - VA ToDo --> 01/07/2025

Type	Code	Description	ECO	STR	P. Risk	R. Risk	VH_ToDo	HI_ToDo	ME_ToDo	LO_ToDo
Cloud Server	SERVER-EQV-AMC	HST-AMC (PORINI)	VH	HI	LO	LO	0	0	0	3
Cloud Server	SERVER-EQV-SUR	HST-SUR (ARUBA)	LW	LW	VH	VH	1	1	2	6
Cloud Server	SERVER-EQV-BME	HST-BME (UNIDATA)	NO	UN	VH	VH	3	1	0	0
Cloud Server	SERVER-EQV-CDP	HST-CDP (ARUBA)	VH	HI	HI	HI	0	1	1	4
Server	SERVER-EQV-10	SRVEQV 10 (Client)	VH	HI	VH	VH	1	1	0	5
Server	SERVER-EQV-60	SRVEQV 60 (DB)	MD	MD	LO	LO	0	0	0	2
Personal Computer	PC-EQV-BEL	PC-EQV-BEL	MD	HI	VH	VH	1	8	4	3
Personal Computer	PC-EQV-TAT	PC-EQV-TAT	NO	HI	VH	VH	1	1	1	4
Server	SRV-EQV	HOST EQV (main)	VH	HI	LO	LO	0	0	0	5
Personal Computer	PC-EQV-DAN	PC-EQV-DAN	NO	MD	VH	VH	0	1	2	5
DeskTop	DSK-EQV-SAN	DSK-EQV-SAN	LW	HI	ME	ME	0	0	2	3
Personal Computer	PC-EQV-CAS	PC-EQV-CAS	NO	MD	VH	VH	1	1	0	0
Personal Computer	PC-EQV-CAR	PC-EQV-CAR	NO	HI	VH	VH	5	2	0	0
Personal Computer	PC-EQV-SAN	PC-EQV-SAN	NO	HI	VH	VH	3	0	1	0
Personal Computer	PC-EQV-LUC	PC-EQV-LUC	NO	LW	HI	HI	0	2	1	0
	CLOUD-EQV-CRA	CLOUD-EQV-CRA			VH	VH	3	8	1	3
Cloud Server	CLOUD-EQV-BME	CLOUD-BME (Aruba)	NO	HI	HI	HI	0	1	0	0

100    200    500

Page 1 of 1 (17 items)

Attività con rischio/impatto *MEDIO* che l'utente «SAN» dovrà eseguire su HW «DSK-EQV-SAN»

**ATTIVITÀ DA ESEGUIRE (PER GRADO DI RISCHIO)**



**ATTIVITÀ DA ESEGUIRE  
(PER GRADO DI RISCHIO)**

Attività con rischio/impatto *MEDIO* che l'utente «SAN» dovrà eseguire su HW «DSK-EQV-SAN»

## DETTAGLIO VULNERABILITÀ

Attività EQV - Assessment    Model HW - Vulnerability Assesse...    Analysys HW - VA ToDo    Periodo 01/07/2025

HW - VA ToDo

Drag a column header here to group by that column

Id	Description	Hardware	Tracking	Severity	Exploit	Malware	Undeleteble	Action
38628	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)	DSK-EQV-SAN	NET	3.00				
38794	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)	DSK-EQV-SAN	NET	3.00				

**HARDWARE INVOLVED**

Involved HW :

Description	Hardware	Action	Action Done
Secure Sockets Layer/Transport La	SERVER-EQV-SUR		
Secure Sockets Layer/Transport La	PC-EQV-BEL		
Secure Sockets Layer/Transport La	PC-EQV-DAN		
Secure Sockets Layer/Transport La	DSK-EQV-SAN		

**ACTION**

Action :

Action Done :

Undeleteble :

Page 1 of 1 (2 items) 1

Page 1 of 1 (4 items) 1

Page 1 of 1 (2 items) 1

25 50 100

ISTRUZIONI / AZIONI RISOLUTIVE (FORNITE DAL MANAGER O SISTEMISTA) E ANNOTAZIONI AZIONI ESEGUITE DA UTENTE

**Risolta la vulnerabilità, l'utente eseguirà il «Check Out» per confermarne la lavorazione**

LISTA HW CON LA STESSA VULNERABILITÀ E AZIONI RISOLUTIVE / AZIONI ESEGUITE

ISTRUZIONI / AZIONI RISOLUTIVE (FORNITE DAL MANAGER O SISTEMISTA) E ANNOTAZIONI AZIONI ESEGUITE DA UTENTE

**Risolta la vulnerabilità, l'utente eseguirà il «Check Out» per confermarne la lavorazione**

Attività EQV - Assessment    Model HW - Vulnerability Assessme...    Analysys VA - User

Attività EQV - Assessment    Model HW - Vulnerability Assessme...    Analysys VA - Hardware    Periodo 01/07/2025

**VA - Hardware**

Drag a column header here to group by that column    VA - Hardware --> 01/07/2025

Code	Description	Severity	Exploit	Malware	Undeleteble	Suspend	Attach	Action	ToDo
38170	SSL Certificate - Subject Common Name Doe...	2.00							10
38173	SSL Certificate - Signature Verification Failed...	2.00							10
38685	SSL Certificate - Invalid Maximum Validity D...	2.00							7
38628	Secure Sockets Layer/Transport Layer Securit...	3.00							
38739	Deprecated SSH Cryptographic Settings	3.00							
38909	SHA1 deprecated setting for SSH	2.00							

100    200    500

**GUIDA RISOLUTIVA**

**FLAG VUNERABILITÀ**

**GRADO IMPATTO / RISCHIO**

**LISTA COMPLETA HW CHE PRESENTA LA VUNERABILITÀ**



# Grazie

## Ulteriori informazioni:

[www.eqv.it](http://www.eqv.it)

## Contatti:

Rino Belloni – CEO

[rino.belloni@eqv.it](mailto:rino.belloni@eqv.it)

Ercole Belloni – Innovation Manager

[ercole.belloni@eqv.it](mailto:ercole.belloni@eqv.it)

