Istituto Comprensivo Statale
BONVESIN DE LA RIVA

COSMI ICF
Condivisione Online Strumenti Modelli Inclusivi

COSMI

una rete per l'inclusione

ACCORDO DI RETE DI SCOPO

L'anno duemila diciotto, sette del mese di NOVEMBRE con il presente atto, da valere a tutti gli effetti di legge, in Legnano alla via Bonvesin 1 , presso la sede dell'Istituzione scolastica Bonvesin de la Riva ,

sono presenti:

	Nominativo del Dirigente Scolastico AMBITO 26	CODICE FISCALE	Legale rappresentate pro-tempore dell'istituzione scolastica (denominazione e codice meccanografico)		Estremi della delibera del Consiglio di Istituto
1	BARBAGLIA DONATA	BRBDNT64M54L669H	LICEO CLASSICO S. QUASIMODO MAGENTA	MIPC140005	
2	BASANO DAVIDE	BSNDVD71L06B041T	ICS CARLO FONTANA MAGENTA	MIIC8FQ00N	
3	BASANO DAVIDE	BSNDVD71L06B041T	LICEO SCIENTIFICO BRAMANTE	MIPS25000Q	
4	BORTOLOTTI ANDREA	BRTNDR58E06F205G	ICS VIA IV NOVEMBRE - CORNAREDO	MIIC8FL00E	
5	BORTOLOTTI ANDREA	BRTNDR58E06F205G	ICS SETTIMO MILANESE	MIIC83200V	N. 59 17/10/2018
6	BREVIGLIERI BARBARA	BRVBBR56A70F205S	I.C. VIA LAMARMORA - LAINATE	MIIC8BC004	
7	CHIODINI GIAMPIERO	CHDGPR57M11E801D	ICS FALCONE E BORSELLINO CASTANO PRIMO	MIIC837002	N. 148 04/10/2018
8	CHIODINI GIAMPIERO	CHDGPR57M11E801D	ICS DON BOSCO INVERUNO	MIIC84100N	N. 135 03/10/2018
9	DAGNINI BRUNO CORRADO	DGNBNC53H21L219Z	ICS RIZZOLI PREGNANA MILANESE	MIIC810002	
10	DRESSINO MARIA CRISTINA	DRSMCR66M71F205J	I.C.S. VIA PAPA GIOVANNI PAOLO II° MAGENTA	MIIC8FR00D	N.54 29/10/2018
11	FASANI GIULIANO	FSNGLN59A06E801F	ICS VIA CAVOUR CUGGIONO	MIIC83800T	N.44 21/11/2018
12	FASANI GIULIANO	FSNGLN59A06E801F	ICS GIORGIO PERLASCA BAREGGIO	MIIC86700T	
13	FRANCONE GIUSEPPA	FRNGPP61B51F881X	ICS TARRA BUSTO GAROLFO	MIIC8DL00N	N. 146 16/10/2018
14	FRANCONE GIUSEPPA	FRNGPP61B51F881X	ICS VILLA CORTESE	MIIC8DK00T	N.87 9/10/2018
15	GNECH AURORA ANNAMARIA	GNCRNN63H60A010Y	IC ALDO MORO CORBETTA	MIIC85600B	N 9 20/12/2018
16	GOTTARDI ALIDA	GTTLMR55T45F205K	ICS MANZONI PARABIAGO	MIIC8FH00N	
17	GOTTARDI ALIDA	GTTLMR55T45F205K	LICEO SCIENTIFICO CAVALERI PARABIAGO	MIPS290006	N. 27 29/10/2018

18	GRASSI ALESSANDRA	GRSLSN60H66H264E	ICS SILVIO PELLICO ARLUNO	MIIC860003	
19	GRASSI ALESSANDRA	GRSLSN60H66H264E	ICS SEDRIANO	MIIC865006I	
20	GRASSI LUCIA	GRSLCU59C62B300X	ICS MANZONI RESCALDINA	MIIC849008	
21	LANDONIO LAURA MARIA LUISA	LNDLMR60S66E514P	IS CARLO DELL'ACQUA LEGNANO	MIIS044009	
22	LAZZATI GABRIELLA	LZZGRL57D48E514Y	ICS MANZONI LEGNANO	MIIC852004	N.67 31/08/2018
23	LAZZATI GABRIELLA	LZZGRL57D48E514Y	ICS CARDUCCI SAN VITTORE	MIIC845001	
24	MALTAGLIATI ANNAMARIA	MLTNMR54L54E801T	I.C. "DUCA D'AOSTA" - OSSONA	MIIC85400Q	N 42 10/10/2018
25	MENNILLI ANNA	MNNNNA57H55B300S	ICS A. STROBINO CERRO	MIIC84700L	N. 82 18/10/2018
26	MENNILLI ANNA	MNNNNA57H55B300S	ICS VIA DEI SALICI LEGNANO	MIIC85500G	N. 28 17/10/2018
27	MEROLA MARIA	MRLMRA60H44D832E	IIS TORNO CASTANO PRIMO	MIIS01200T	N 29 24/11/2018
28	MEROLA MARIA	MRLMRA60H44D832E	I.C. ADA NEGRI MAGNAGO	MIIC84200D	N. 4 25/10/2018
29	OLIVARI SARA	LVRSRA66S60A940V	LICEO CLEMENTE REBORA RHO	MIPC13000E	N. 66 15/10/2018
30	OSNAGHI ELENA	SNGLNE64H67D198J	ICS BONVESIN DE LA RIVA LEGNANO	MIIC8D9008	N 52 11/10/2018
31	OSNAGHI ELENA	SNGLNE64H67D198J	ICS CARDUCCI LEGNANO	MIIC8EA008	N.35 30/10/2018
32	PISONI MARIA GRAZIA	PSNMGR61M46E801F	ICS "E. DE AMICIS" MARCALLO	MIIC858003	
33	PISONI MARIA GRAZIA	PSNMGR61M46E801F	IIS LUIGI EINAUDI MAGENTA	MIIS09100V	
34	PURICELLI ERMANNO	PRCRNN53D19B286T	OMNICOMPRENSIVO ARCONATE	MIIC84000T	26/11/2018
35	SILANOS MARIA	SLNMRA72C53B300E	ICS DON L. MILANI TURBIGO	MIIC836006	N. 126 30/10/2018
36	TERRONE GIUSEPPE	TRRGPP54R07B619N	ICS VIALE LEGNANO PARABIAGO	MIIC8FG00T	N. 85 26/10/2018
37	TERRONE GIUSEPPE	TRRGPP54R07B619N	ICS NERVIANO	MIIC85300X	N. 102 29/10/2018
38	WAGNER ANNALISA	WGNNLS64L70L682X	I.S.I.S. A. BERNOCCHI LEGNANO	MIIS09700T	N. 161 DEL 22/10/2018
	Nominativo del Dirigente Scolastico ALTRI AMBITI	**CODICE FISCALE**	**Legale rappresentate pro-tempore dell'istituzione scolastica (denominazione e codice meccanografico)**		**Estremi della delibera del Consiglio di Istituto**
1	LIBRALATO ELISABETTA	LBRLBT62L57E625Q	IC DELLA MARGHERITA VIZZOLO PREDABISSI	MIIC8A300D	N82 22/11/2018

Premesso Che l'art. 7 del DPR n. 275/1999 prevede che le istituzioni scolastiche possono promuovere accordi di rete o aderire ad essi per il raggiungimento delle proprie finalità istituzionali e che gli accordi sono aperti all'adesione di tutte le istituzioni scolastiche che intendano parteciparvi e prevedono iniziative per favorire la partecipazione alla rete delle istituzioni scolastiche che presentano situazioni di difficoltà;

Premesso Che l'art. 15 della legge 7 agosto 1990, n. 241 prevede che le amministrazioni pubbliche possono concludere tra loro accordi per disciplinare lo svolgimento in collaborazione di attività di interesse comune;

Premesso Che l'art. 1 comma 70 della legge 13 luglio 2015, n 107 dispone che gli Uffici scolastici regionali promuovano la costituzione di reti tra istituzioni scolastiche del medesimo ambito;

Viste Le Linee guida adottate dal Ministero dell'Istruzione, dell'Università e della Ricerca con nota MIUR 07.06.2016, PROT. N. 2151

Considerato Che detta rete di ambito ha tra l'altro lo scopo di facilitare la costituzione di reti (reti di scopo) per la valorizzazione e formazione delle risorse professionali, la gestione comune di funzioni e di attività amministrative, nonché la realizzazione di progetti o di iniziative didattiche, educative, sportive o culturali di interesse territoriale nel medesimo ambito territoriale;

Considerato Che le istituzioni scolastiche sopraddette hanno interesse a collaborare reciprocamente per l'attuazione di iniziative comuni;

Considerato Che tale collaborazione è finalizzata:

- alla miglior realizzazione della funzione della scuola come centro di educazione ed istruzione, nonché come centro di promozione culturale, sociale e civile del territorio;
- al completamento e miglioramento dell'iter del percorso formativo degli alunni, in particolare degli alunni DVA;
- a favorire una comunicazione più intensa e proficua fra le istituzioni scolastiche;
- a stimolare e a realizzare, anche attraverso studi e ricerche, l'accrescimento della qualità dei servizi offerti dalle istituzioni scolastiche;

Verificato Che le Istituzioni Scolastiche sopra menzionate hanno interesse a collaborare reciprocamente per l'attuazione di iniziative comuni afferenti agli obiettivi sopra citati.

i sopraddetti con il presente atto convengono quanto segue:

Art. 1

Norma di rinvio

La premessa e gli allegati costituiscono parte integrante e sostanziale del presente accordo.

Art. 2

Definizioni

Per Istituzioni Scolastiche aderenti si intendono le Istituzioni scolastiche che sottoscrivono il presente accordo e quelle che vi aderiscono anche successivamente.

Art. 3

Denominazione della rete

Viene costituito e istituito il collegamento in rete tra le Istituzioni scolastiche firmatarie del presente accordo, che assume la denominazione di **COSMI – UNA RETE PER L'INCLUSIONE**, con scuola capofila ICS BONVESIN DE LA RIVA di Legnano.

Art. 4

Oggetto

Il presente accordo ha ad oggetto la collaborazione fra le istituzioni scolastiche aderenti per la progettazione ed realizzazione delle seguenti attività:

- *Utilizzo della piattaforma COSMI.ICF per la stesura/compilazione del PEI in chiave ICF e con la partecipazione di tutti i soggetti coinvolti nel Progetto di vita degli alunni DVA.*
- *Diffusione del sistema di classificazione ICF-CY come linguaggio condiviso per la definizione del Profilo di Funzionamento, attraverso l'individuazione di processi e sottoprocessi atti a fornire la comprensione più approfondita possibile dell'alunno*
- *Realizzazione di un servizio di consulenza, formazione e supporto operativo da parte di docenti del gruppo di progetto.*

Art. 5

Progettazione e gestione delle attività

Al fine della realizzazione delle attività di cui al precedente art. 4, le istituzioni scolastiche aderenti al presente accordo specificano in concreto le attività oggetto della reciproca collaborazione.
A tal fine, viene predisposto, un "progetto" nel quale sono individuate analiticamente le attività da porre in essere e la concrete finalità cui le stesse si indirizzano, con indicazione:
a) delle attività istruttorie e di gestione;
b) delle risorse professionali (interne o esterne)
c) delle risorse finanziarie e della loro ripartizione fra le istituzioni scolastiche aderenti o coinvolte;
d) dell'istituzione scolastica incaricata della gestione delle attività amministrative e contabili, individuata sin da ora nell'Istituzione scolastica **ICS BONVESIN DE LA RIVA di Legnano**, che assume la funzione di "Scuola capo-fila" per la realizzazione del progetto;
e) delle attività di monitoraggio.
Le attività istruttorie comprendono, fra le altre, tutte le attività di progettazione (di massima o esecutiva), di proposta, di acquisizione di informazioni o documentazione, di istruttoria vera e propria nell'ambito dei procedimenti di scelta del contraente.
Le attività di gestione comprendono le attività di attuazione tecnico-professionale e le attività di attuazione amministrativa.
Le attività di gestione amministrativa comprendono sia le attività deliberative che le attività meramente esecutive.
Il progetto di cui al presente articolo deve essere approvato dalla conferenza dei dirigenti scolastici della rete, di cui all'art. 5, nonché, ove siano coinvolte materie rientranti nell'ambito della competenza degli

organi collegiali (Collegio dei docenti e Consiglio d'Istituto) delle singole istituzioni scolastiche, anche dai competenti organi delle istituzioni scolastiche aderenti e coinvolte dall'attività oggetto del progetto.

Art. 5

Conferenza dei dirigenti scolastici della rete di scopo

Al fine della realizzazione delle attività progettate, i dirigenti scolastici delle istituzioni scolastiche aderenti al presente accordo si riuniscono al fine di:

a) determinare l'ammontare di un fondo spese per il generale funzionamento amministrativo della "rete" e la ripartizione dello stesso fra le istituzioni scolastiche aderenti, da versare all'istituzione scolastica capo-fila;

b) approvare il progetto di cui all'art. 4;

c) adottare ogni determinazione rientrante nell'autonoma competenza di gestione del dirigente scolastico, che risulti necessaria all'attuazione dei progetti di cui all'art. 4;

d) adottare ogni altra determinazione, previa acquisizione delle deliberazioni degli organi collegiali competenti.

La conferenza dei dirigenti scolastici opera come conferenza di servizi ai sensi dell'art. 14 della L. 7 agosto 1990, n. 241 e successive modificazioni ed integrazioni.

La conferenza dei dirigenti scolastici è convocata dal dirigente scolastico preposto all'istituzione scolastica capo-fila.

Art.6

Finanziamento e gestione amministrativo-contabile

Con riguardo alla gestione delle attività amministrative e contabili, l'istituzione scolastica capofila acquisirà al proprio bilancio il finanziamento destinato all'attuazione del progetto, pari a euro 100 per ogni istituzione aderente alla rete in oggetto, quale entrata finalizzata allo stesso.

L'invio delle credenziali di accesso alla piattaforma è subordinato al pagamento della quota di partecipazione e all'invio del mandato emesso (Conto tesoreria unica num. 313176 codice tesoreria 139 causale "Adesione rete COSMI 2018-2019").

L'istituzione scolastica capo-fila porrà in essere, attraverso i propri uffici, tutte le attività istruttorie necessarie, ivi comprese quelle afferenti ai procedimenti di scelta del contraente.

Le attività di gestione amministrativa di tipo deliberativo vengono adottate secondo le modalità richiamate nell'art. 5, lett. c) e d).

La gestione amministrativo-contabile è oggetto di analitica rendicontazione, parziale e/o finale, in base alle scadenze individuate nella allegata Scheda tecnica.

La destinazione degli eventuali saldi attivi è determinata dalla conferenza dei dirigenti scolastici della rete di scopo secondo le modalità richiamate nell'art. 5, letto c) e d).

Allo stesso modo è amministrato il fondo spese annuale per il generale funzionamento amministrativo della **Rete COSMI** da parte dell'istituzione scolastica a ciò incaricata, che è tenuta ad una rendicontazione finale.

In ogni momento, comunque, gli organi delle altre istituzioni scolastiche possono esercitare il diritto di accesso ai relativi atti.

Art.7

Impiego del personale

L'individuazione delle risorse professionali interne e la distribuzione delle attività tecnico-professionali fra il personale delle istituzioni scolastiche aderenti al presente accordo è contenuto nella allegata Scheda tecnica, fermo il rispetto delle disposizioni legislative vigenti.

Art. 8

Durata

Il presente accordo ha validità dalla data di sottoscrizione al 31 agosto 2019.
Non è ammesso il rinnovo tacito.

Art. 9

Modalità di adesione

La richiesta di adesione al presente accordo va proposta con dichiarazione del Dirigente scolastico, resa in forma pubblica e trasmessa con la delibera del Consiglio di Istituto alla Conferenza dei servizi, presso la sede della scuola capofila. L'adesione ha effetto dal momento della formale sottoscrizione dell'accordo da parte dell'Istituzione scolastica richiedente.

Art. 10

Modalità di recesso

Le Istituzioni scolastiche aderenti hanno facoltà di recesso dal presente accordo. Il recesso è esercitato tramite dichiarazione del Dirigente scolastico, resa in forma pubblica e trasmessa con la delibera del Consiglio di Istituto alla Conferenza dei servizi.

Art. 11

Norme finali

L'accordo viene inviato alle scuole aderenti. Lo stesso è pubblicato all'albo e depositato presso l'Ufficio di segreteria delle scuole aderenti. Gli interessato potranno prenderne visione ed estrarne copie. Per quanto non espressamente previsto nel presente atto, si rimanda all'Ordinamento generale in materia di istruzione ed alle norme che regolano il rapporto di lavoro nel comparto Scuola.

	Nominativo del Dirigente Scolastico AMBITO 26	Codice Meccanografico	Firma
1	BARBAGLIA DONATA	MIPC140005	
2	BASANO DAVIDE	MIIC8FQ00N	
3	BASANO DAVIDE	MIPS25000Q	
4	BORTOLOTTI ANDREA	MIIC8FL00E	
5	BORTOLOTTI ANDREA	MIIC83200V	

6	BREVIGLIERI BARBARA	MIIC8BC004	
7	CHIODINI GIAMPIERO	MIIC837002	
8	CHIODINI GIAMPIERO	MIIC84100N	
9	DAGNINI BRUNO CORRADO	MIIC810002	
10	DRESSINO MARIA CRISTINA	MIIC8FR00D	
11	FASANI GIULIANO	MIIC83800T	
12	FASANI GIULIANO	MIIC86700T	
13	FRANCONE GIUSEPPA	MIIC8DL00N	
14	FRANCONE GIUSEPPA	MIIC8DK00T	
15	GNECH AURORA ANNAMARIA	MIIC85600B	
16	GOTTARDI ALIDA	MIIC8FH00N	
17	GOTTARDI ALIDA	MIPS290006	
18	GRASSI ALESSANDRA	MIIC860003	
19	GRASSI ALESSANDRA	MIIC865006I	
20	GRASSI LUCIA	MIIC849008	
21	LANDONIO LAURA MARIA LUISA	MIIS044009	
22	LAZZATI GABRIELLA	MIIC852004	
23	LAZZATI GABRIELLA	MIIC845001	
24	MALTAGLIATI ANNAMARIA	MIIC85400Q	
25	MENNILLI ANNA	MIIC84700L	
26	MENNILLI ANNA	MIIC85500G	
27	MEROLA MARIA	MIIS01200T	
28	MEROLA MARIA	MIIC84200D	
29	OLIVARI SARA	MIPC13000E	

30	OSNAGHI ELENA	MIIC8D9008	
31	OSNAGHI ELENA	MIIC8EA008	
32	PISONI MARIA GRAZIA	MIIC858003	
33	PISONI MARIA GRAZIA	MIIS09100V	
34	PURICELLI ERMANNO	MIIC84000T	
35	SILANOS MARIA	MIIC836006	
36	TERRONE GIUSEPPE	MIIC8FG00T	
37	TERRONE GIUSEPPE	MIIC85300X	
38	WAGNER ANNALISA	MIIS09700T	
	Nominativo del Dirigente Scolastico AMBITO 25	**Firma**	**Firma**
1	LIBRALATO ELISABETTA	MIIC8A300D	

ALLEGATI

1. SCHEDA TECNICA
2. Dati sicurezza informatica
3. Elenco Aggiuntivo

Istituto Comprensivo Statale
BONVESIN DE LA RIVA

COSMI ICF
Condivisione Online Strumenti Modelli Inclusivi

SCHEDA TECNICA

Progetto: COSMI – IN RETE PER L'INCLUSIONE

Descrizione e finalità	Compilazione on line del Piano Educativo Individualizzato in chiave ICF, condivisa con tutti gli operatori dell'inclusione degli alunni DVA, per realizzare il Progetto di vita come previsto dagli'art.6 e 7 dlgs 66/2017
Azioni ente capofila	- Verifica della funzionalità della piattaforma in termini di adeguatezza ai bisogni - Miglioramento costante della sua operatività - Monitoraggio continuo della sicurezza dei dati tramite affidamento ad ente certificatore esterno - Assegnazione ai legali rappresentanti delle istituzioni scolastiche aderenti delle credenziali per poter abilitare i propri docenti, genitori, educatori ed eventualmente terapisti della riabilitazione - Ampliamento del portale con sezioni di assistenza on line e approfondimenti, consulenza specifica
Azioni delle scuole aderenti	- Gestione degli accessi alla piattaforma per la parte di propria competenza - Segnalazione immediata alla scuola capofila di eventuali problemi legati alla funzionalità e alla sicurezza
Risorse professionali	**Personale interno (gruppo di progetto)** - per la parte tecnica: ✓ Ins. Fumante Mariano - per la parte specifica dei contenuti della piattaforma ✓ Ins. De Luca Katia ✓ Ins. Valota Roberto ✓ Ins. Mantegazza Francesca **Personale esterno** - Wom srl per la parte informatica - Data Security per la protezione dei dati e la sicurezza
Gestione delle attività amministrativo -contabili	Dott. Balotta Antonio in qualità di Dsga Assistente amministrativo da individuare
Coordinamento del progetto	Prof. De Luca Katia
Monitoraggio e coordinamento tecnico	Prof. Fumante Mariano

Istituto Comprensivo Statale
BONVESIN DE LA RIVA

COSMI ICF
Condivisione Online Strumenti Modelli Inclusivi

ELENCO AGGIUNTIVO

	Nominativo del Dirigente Scolastico AMBITO 26	CODICE FISCALE	Legale rappresentate pro-tempore dell'istituzione scolastica (denominazione e codice meccanografico)		Estremi della delibera del Consiglio di Istituto
1	GIUSEPPINA TIANA ALOISI	LSAGPP72L47F205K	MIIC8FK00P	ICS DA VINCI CORNAREDO	N.104 27/11/2018
2	VITTORIO Michela	VTTMHL54M50D969T		IS Rueca Oliveti	
3	MARCELLO BETTONI	BTTMCL59R20D112C	MIPS13000N	LICEO SCIENT. N.5 GALILEI LEGNANO	9/11/2018
4	LAZZATI DANIELA	LZZDNL54S46F205B	MITD57000B	ITET G. MAGGIOLINI	
5	"	"	MITF13000Q	ITT CANNIZZARO	
6	MORONI SANDRA	MRNSDR59P43H264E	MIIC8FF002	I.C. TOMMASO GROSSI RHO	
7	MORONI SANDRA	MRNSDR59P43H264E	MIIC8GD001	I.C. EZIO FRANCESCHINI RHO	
	~~ALIDA~~ MARINA ~~VGOTTARDI~~	~~GTTLMR65T45F205K~~			
8	FIORELLINO MARISA	FRLMRS52P69F839J	MIIS08300X	MENDEL VILLA C.	25/10/2018
9	FIORELLINO MARISA	FRLMRS52P69F839J	MIIS016005	IIS INVERUNO	
	~~GARRON~~				
10	TIANA M. TERESA	TNIMTR61H63F205C	MIIC8EB004	IC EUROPA UNITA ARESE	
11	LAMARI MARIA	LMRMRA56S62Z104Y	MITD52000A	IT MATTEI RHO	
12	CALDARULO ROSSANA	CLDRSN63C47F205C	MIIC8EC00X	IC DON GNOCCHI	N72 2018
13	GUZZO GIULIANA	CVALLO CVL GLN58C44 G677Z	MIIC8B1007	ICS PERO	
14	~~GIURANNA~~				

	Nominativo del Dirigente Scolastico ALTRI AMBITI	CODICE FISCALE	Legale rappresentate pro-tempore dell'istituzione scolastica (denominazione e codice meccanografico)		Estremi della delibera del Consiglio di Istituto
1	GARRONI ROBERTO	GRRRRT58T21Z602K	ICS IQBAL PIOLTELLO	MIIC88L00C	N 1 8/11/2018
2	GIURANNA FRANCESCA		LIS MONTALE	MIIS02800B	
3	GIOVANNA RUGGERI	RGGGNN60R65I566O	IC DANTE UITUONE	MIIC862	00P

	Nominativo del Dirigente Scolastico AMBITO 26	Codice Meccanografico	Firma
1	GIUSEPPINA T. ALOISI	TIIC8FK00P	
2	VITTORIO	MIIS08900V	
3	BETTONI	MIPS13000N	
4	LAZZATI Daniela	MITD5[illegible]0003	
5	" "	MITF13000Q	
6	SANDRA MORONI	MIIC8FF002	
7	SANDRA MORONI	MIIC8GD001	
8	FIORELLINO MARISA	MIIS08300X	
9	FIORELLINO MARISA	MIIS01600S	
10	TIANA M. TERESA	MIIC8EB004	
11	LAMARI MARIA	MITD52000A	

12	CALDARULO ROSSANA	MIIC8EC00X	
13	CAVALLO GOZZO GIULIANA	MIIC8BT007	

	Nominativo del Dirigente Scolastico ALTRI AMBITI	Codice Meccanografico	Firma
	GARRONI ROBERTO	MIIC8BL00C	
	GIURANNA FRANCESCA	MIIS02800B	
	RUGGERI GIOVANNA	MIIC86200P	

Qualys. Consultant

Scan Results

October 23, 2018

Report Summary	
User Name:	Giancarlo Favero
Login Name:	
Company:	ISwisstech Srl - Data Security
User Role:	Manager
Address:	
City:	
Zip:	
Country:	Italy
Created:	10/23/2018 at 06:57:19 (GMT)
Client:	
Launch Date:	10/22/2018 at 12:18:48 (GMT)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1540210728.22058
External Scanners:	154.59.121.146 (Scanner 10.4.47-1, Vulnerability Signatures 2.4.446-2)
Duration:	08:13:39
Title:	CosmiICF
Asset Groups:	-
IPs:	89.46.71.245
Excluded IPs:	-
Options Profile:	Initial Options

Summary of Vulnerabilities

Vulnerabilities Total	16	Security Risk (Avg)	1.0

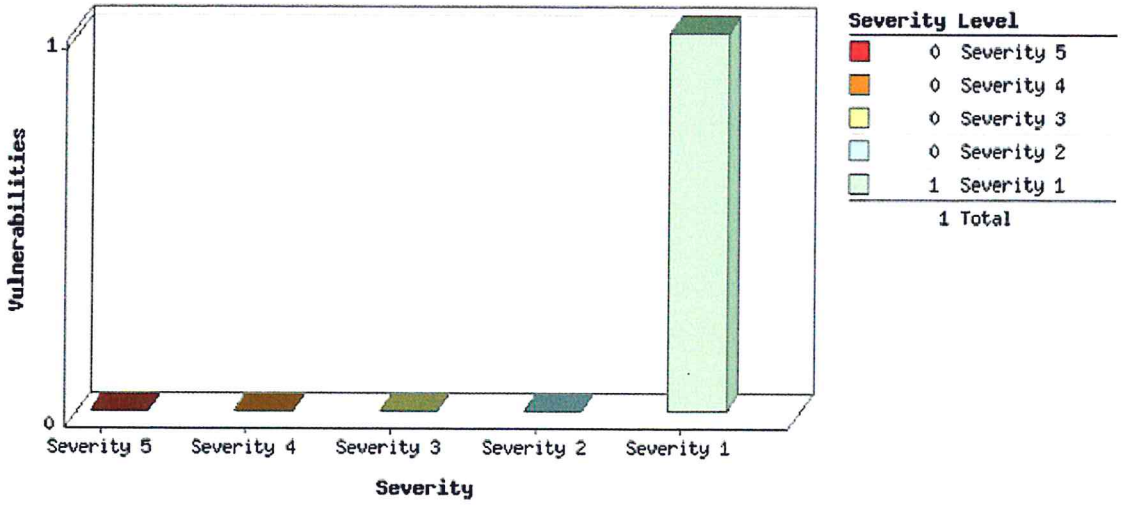
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	0	1	1
2	0	0	3	3
1	1	1	10	12
Total	1	1	14	16

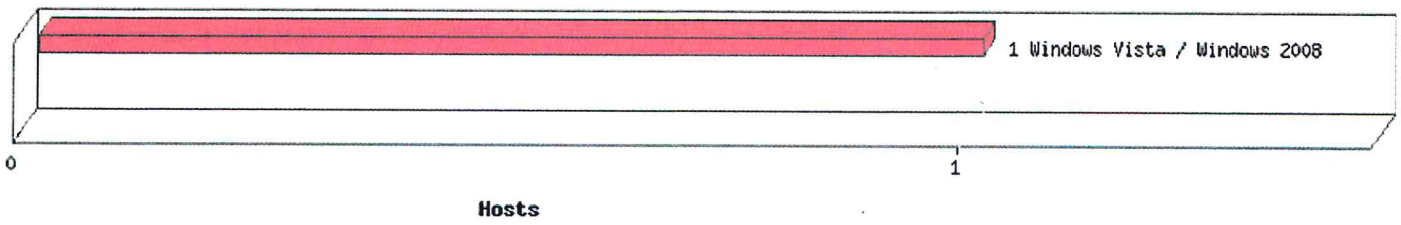
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
Information gathering	1	0	6	7
TCP/IP	0	0	4	4
General remote services	0	1	1	2
Web server	0	0	1	1
Firewall	0	0	1	1
Total	1	1	13	15

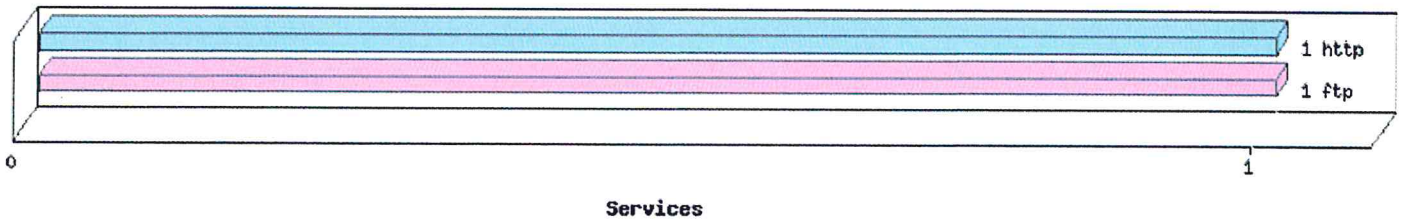
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

89.46.71.245 (host245-71-46-89.serverdedicati.aruba.it, -) Windows Vista / Windows 2008

Vulnerabilities (1)

1 Remote Management Service Accepting Unencrypted Credentials Detected

QID:	45242
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/08/2018
User Modified:	-

Edited:	No
PCI Vuln:	Yes

THREAT:
A remote management service that accepts unencrypted credentials was detected on target host.
Services like Telnet, FTP, HTTP with basic auth are checked.
Services like TFTP are also checked.

IMPACT:
A malicious individual can easily intercept unencrypted passwords during transmission using a "network sniffer" and use this data to gain unauthorized access.

SOLUTION:
If possible, use alternate services that provide encryption.
Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Service name: FTP on TCP port 21.

Potential Vulnerabilities (1)

1 Possible Scan Interference

QID:	42432
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
Possible scan interference detected.
A PCI scan must be allowed to perform scanning without interference from intrusion detection systems or intrusion prevention systems.
The PCI ASV is required to post fail if scan interference is detected.
The goal of this QID is to ensure that Active Protection Systems are not blocking, filtering, dropping or modifying network packets from a PCI Certified Scan, as such behavior could affect an ASV's ability to detect vulnerabilities. Active Protection Systems could include any of the following; IPS, WAF, Firewall, NGF, QoS Device, Spam Filter, etc. which are dynamically modifying their behavior based on info gathered from traffic patterns.
This QID is triggered if a well known and popular service is not identified correctly due to possible scan interference. Services like FTP, SSH, Telnet, DNS, HTTP and Database services like MSSQL, Oracle, MySql are included.
-If an Active Protection System is found to be preventing the scan from completing, Merchants should make the required changes (e.g. whitelist) so that the ASV scan can complete unimpeded.
-If the scan was not actively blocked, Merchants can submit a PCI False Positive/Exception Request with a statement asserting that No Active Protection System is present or blocking the scan.
Additionally, if there is no risk to the Cardholder Data Environment, such as no web service running, this can also be submitted as a PCI False Positive/Exception Request and reviewed per the standard PCI Workflow.
For more details on scan interference during a PCI scan please refer to ASV Scan Interference section of PCI DSS Approved Scanning Vendors Program Guide Version 2.0 May 2013 - page 14/28 (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v2.pdf).

IMPACT:

If the scanner cannot detect vulnerabilities on Internet-facing systems because the scan is blocked by an IDS/IPS, those vulnerabilities will remain uncorrected and may be exploited if the IDS/IPS changes or fails.

SOLUTION:
Whitelist the Qualys scanner to scan without interference from the IDS or IPS.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Service name: Unknown - Possible Scan Interference on TCP port 443.

Information Gathered (14)

3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/26/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.
The Results section includes information on the remote access service that was found on the target.
Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Service name: FTP on TCP port 21.

2 Operating System Detected

QID: 45017

Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable.

SOLUTION:
Not applicable.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows Vista / Windows 2008	TCP/IP Fingerprint	U3414:21

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in

various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Based on TCP timestamps obtained via port 21, the host's uptime is 67 days, 20 hours, and 32 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

2 FTP Server Banner

port 21/tcp

QID:	27113
Category:	File Transfer Protocol
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/25/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following message is shown to all users logging on to your FTP server, including anonymous logins if they are allowed on your server.

IMPACT:
Unauthorized users can obtain sensitive information about your server, such as the version or type of server you are running, and use this information to implement specific attacks against the server.

SOLUTION:
If possible, edit the configuration files or recompile the server to restrict the type of information disclosed.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
220 FileZilla Server 0.9.59 beta

1 DNS Host Name

QID:	6
Category:	Information gathering

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
89.46.71.245	host245-71-46-89.serverdedicati.aruba.it

 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/16/2001
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Some of the ports filtered by the firewall are: 20, 22, 23, 25, 53, 111, 135, 445, 1, 7.

Listed below are the ports filtered by the firewall.

No response has been received when any of these ports are probed.
1-3,5,7,9,11,13,15,17-20,22-25,27,29,31,33,35,37-39,41-79,81-223,242-246,
256-265,280-282,309,311,318,322-325,344-351,363,369-442,444-581,587,592-593,
598,600,606-620,624,627,631,633-637,666-674,700,704-705,707,709-711,729-731,
740-742,744,747-754,758-765,767,769-777,780-783,786,799-801,860,873,886-888,
900-901,911,950,954-955,990-993,995-1001,1008,1010-1011,1015,1023-1100,
1109-1112,1114,1123,1155,1167,1170,1207,1212,1214,1220-1222,1234-1236,
1241,1243,1245,1248,1269,1313-1314,1337,1344-1625,1636-1705,1707-1774,
1776-1815,1818-1824,1900-1909,1911-1920,1944-1951,1973,1981,1985-1999,
2001-2028,2030,2032-2036,2038,2040-2049,2053,2065,2067,2080, and more.
We have omitted from this list 706 higher ports to keep the report size manageable.

 1 Internet Service Provider

QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
The ISP network handle is: RIPE-C3
ISP Network description:
RIPE Network Coordination Centre

 1 Traceroute

QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	154.59.121.130	0.13ms	ICMP	
2	149.14.140.97	0.80ms	ICMP	
3	154.54.37.97	1.96ms	ICMP	
4	130.117.0.142	7.98ms	ICMP	
5	154.54.36.54	12.83ms	ICMP	
6	130.117.0.61	18.11ms	ICMP	
7	154.54.38.102	22.99ms	ICMP	
8	154.54.59.1	26.93ms	ICMP	
9	130.117.48.114	33.53ms	ICMP	
10	149.6.18.50	32.85ms	ICMP	
11	62.149.185.59	31.99ms	ICMP	
12	*.*.*.*	0.00ms	Other	80
13	89.46.71.245	32.15ms	TCP	80

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Scan duration: 29606 seconds

Start time: Mon, Oct 22 2018, 10:23:28 GMT

End time: Mon, Oct 22 2018, 18:36:54 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/14/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
host245-71-46-89.serverdedicati.aruba.it	FQDN

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
21	ftp	File Transfer [Control]	ftp	
80	www-http	World Wide Web HTTP	http	
443	https	http protocol over TLS/SSL	unknown	

1 Degree of Randomness of TCP Initial Sequence Numbers

QID: 82045
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/19/2004
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Average change between subsequent TCP initial sequence numbers is 1281223407 with a standard deviation of 606563296. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(4995 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
IP ID changes observed (network order) for port 21: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 30 milli seconds

1 Web Server Version port 80/tcp

QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/26/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
N/A

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Server Version	Server Banner
Microsoft-HTTPAPI/2.0	Microsoft-HTTPAPI/2.0

Appendix

Hosts Scanned (IP)

89.46.71.245

Target distribution across scanner appliances

External : 89.46.71.245

Options Profile

Initial Options

Scan Settings

Ports:	
Scanned TCP Ports:	Standard Scan
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Load Balancer Detection:	Off
Perform 3-way Handshake:	Off
Vulnerability Detection:	Complete
Password Brute Forcing:	
System:	Disabled
Custom:	Disabled
Authentication:	
Windows:	Disabled
Unix/Cisco:	Disabled
Oracle:	Disabled
Oracle Listener:	Disabled
SNMP:	Disabled
VMware:	Disabled
DB2:	Disabled
HTTP:	Disabled
MySQL:	Disabled
Tomcat Server:	Disabled
MongoDB:	Disabled
Palo Alto Networks Firewall:	Disabled
Jboss Server:	Disabled
Oracle WebLogic Server:	Disabled
MariaDB:	Disabled
Overall Performance:	Normal
Authenticated Scan Certificate Discovery:	Disabled
Test Authentication:	Disabled
Hosts to Scan in Parallel:	
Use Appliance Parallel ML Scaling:	Off
External Scanners:	15
Scanner Appliances:	30
Processes to Run in Parallel:	
Total Processes:	10
HTTP Processes:	10
Packet (Burst) Delay:	Medium
Port Scanning and Host Discovery:	

Intensity:	Normal
Dissolvable Agent:	
Dissolvable Agent (for this profile):	Disabled
Windows Share Enumeration:	Disabled
Windows Directory Search:	Disabled
Lite OS Discovery:	Disabled
Host Alive Testing:	Disabled
Do Not Overwrite OS:	Disabled

Advanced Settings

Host Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore firewall-generated TCP RST packets:	Off
Ignore all TCP RST packets:	Off
Ignore firewall-generated TCP SYN-ACK packets:	Off
Do not send TCP ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include

Severity	Level	Description
		full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.

Ds Elena Osnaghi
11/01/2019 14:38:27