ACME Company
Report Dettagliato

Nome dello Scan: Fred_-_company_website_

Eseguito il 2022-08-19 14:17:26

Riservato

Indice

Introduzione

Questo report è il risultato di un "online vulnerability assessment", es

Questo documento è stato redatto e predisposto per fornire u
comprensione per semplificare il compito di mettere in si
apparecchiature informatiche collegate a Internet.

Le vulnerabilità di sistema sono classificate in base a Autore, Data
Informazioni. Una spiegazione dettagliata per ciascuna categoria di vuln
Livelli di gravità.

Un Executive Summary è stato redatto appositamente per una cons
management. Questo contiene sia informazioni scritte sia grafi
vulnerability assessment. Tali risultati includono informazioni
scansione", "chi ha eseguito la scansione", e la quantità di vu
categoria.

L'Executive Summary include anche una conclusione che riporta il "livello c
del sistema sotto esame.

I dettagli e nomi delle vulnerabilità trovate si trovano nella tabella
seguire, sono elencati i dettagli di ciascuna vulnerabilità e le indicaz

Dove possibile, sono specificati ID Bugtraq (*), CVE (**) o USN (***) per una ricerca
approfondita.

Ogni vulnerabilità individuata viene corredata con un possibile rimedi

(*) Bugtraq ID è l'ID ufficiale di Securityfocus.com; Conosciuto anche come Bugtraq.
(**) CVE è l'elenco ufficiale CVE Mitre.
(***) USN è la lista ufficiale di Ubuntu Security Notice.

Livelli di gravità

Vulnerabilità di livello Alto

Quando viene individuata una vulnerabilità di livello Alto, signiû c
penetrare e compromettere completamente il sistema e/o accede
sensibili. Esiste un elevato rischio di furto o perdita di dati privati e

Vulnerabilità di livello Medio

Quando viene individuata una vulnerabilità di livello Medio, signiû
l'accesso a informazioni di sistema che potrebbero portare ad attacch
alla compromissione del sistema. Ciò a sua volta potrebbe portare al
e sensibili.

Vulnerabilità di livello Basso

Quando viene individuata una vulnerabilità di livello Basso, signiû ca
ottenere l'accesso a informazioni di sistema che possono aiutare a co
conseguente furto o perdita di dati privati e sensibili.

Informazione

Tutte le voci di livello Informazione forniscono semplicemente info
disponibili sul sistema in esame. Non costituiscono un'indicazion
sistema.

Executive Summary

Questo report illustra il risultato di una scansione di Sicurezza ACME Company. Contiene informazioni riservate sullo stato della rete. L'accesso a personale non autorizzato può consentire loro di compromettere la sic

Nome dello Scan	Fred_-_company_website_scan	Profilo di scansione	Wordpress
Data/ora Inizio	2022-08-19 14:17:26	Data/ora fine	2022-08-19 14:19:57
Durata	00:02:31 (2 minutes, 31 seconds)		
Versione Scanner	9.9.33.1022	No translation available for: "Firmware Version"	54.0.4
Elenco dei siste controllati	dv.it		

Questa scansione è stata eseguita manualmente dall'utente

Livello di Sicurezza Complessivo

Cat. 2 (livello Medio)

La scansione eseguita da ACME Company ha determinato che sicurezza del sistema è ad un livello medio paralizzare il sistema in modo da portare ad un pe del sistema e/o portare attacchi più gravi. Si rac provvedimenti immediati per aumentare il livello di

Sistemi Online

Tutti i sistemi erano in linea al momento della scansione.

Sistemi Offline

La scansione non ha individuato nessun sistema scollegato.

Analisi dei Risultati

Un totale di 2 potenziali vulnerabilità sono state individuate nei sist
rapporto 0.0% di vulnerabilità di livello Alto.

Numero totale di vulnerabilità

Elenco delle porte più vulnerabili, in base al numero di vulnerabilità r

Traceroute

Questo è il risultato di una traceroute da ACME Company ai sistemi es

traceroute to 35.214.203.110 (35.214.203.110), 15 hops max, 60 byte

Hop	Nome	IP	Località	Med(ms)	Graû co
1	192.168.90.1	192.168.90.1		1.973	
2	*	*	-	-	-
3	172.17.121.48	172.17.121.48		7.849	
4	172.17.120.140	172.17.120.140		9.040	
5	172.19.184.52	172.19.184.52		16.100	
6	172.19.177.24	172.19.177.24		14.821	
7	ae48.milano11.mil.seabone.net	195.22.192.144	Italy	11.543	
8	ae5.francoforte34.fra.seabone.net	195.22.196.17	Italy	32.630	
9	195.219.223.10	195.219.223.10		27.101	
10	if-ae-9-2.tcore1.fnm-frankfurt.as6453.net	5.23.63.16		33.196	
11	*	*	-	-	-
12	if-ae-7-4.tcore1.ad1-amsterdam.as6453.net	80.231.154.58		32.680	
13	195.219.150.29	195.219.150.29		31.467	
14	59.223.214.35.bc.googleusercontent.com	35.214.223.59	United States(MI) Ann Arbor	37.459	
15	110.203.214.35.bc.googleusercontent.com	35.214.203.110	United States(MI) Ann Arbor	35.410	

Porte e servizi individuati

Le seguenti porte e servizi sono state individuate sui sistemi esamina

Porte e Serviz ɔianoodv.it

Nessuna Porta o Servizio individuati su questo sistema.

Segnalatori di Versione individuati

I seguenti Segnalatori di Versione (Version Banner) sono stati letti su
Si consiglia vivamente di riconûgurare questi segnalatori con i
informazione aû atto.

Segnalatori di Versi	ianoodv.it
Nessuno	

Nessun Segnalatore di Versione è stato individuato.

Elenco delle Vulnerabilità

Sistema Ta ıoodv.it

Livello rischio	Vulnerabilità
	Domain DMARC Value Missing
	Remote system answers to PING command

Vulnerabilità

Sistema Ta ınoodv.it

Vulnerabilità	Domain DMARC Value Missing
Livello rischio	Medio
Porta	443/tcp
SPID	61917
Impatto	The target domain is missing DMARC value. DMARC utilizes SPF and DKIM authenticates properly. DMARC can also ensure fraudulent emails attempt blocked. To pass DMARC checks, an email must pass SPF authentication a authentication and DKIM alignment. DMARC ultimately allows the organiza decide how receiving email servers should handle messages that fail DMA or reject. Similar to SPF and DKIM, DMARC also leverages DNS for its fur implementation process is rather easy, although the full process can take Before starting a DMARC implementation, the administrator must identify receive the daily XML reports. Using a ch as postmaster acceptable for most domains.
Output della vulnerabilità / Evidenze	
	Missing DMARC value

Vulnerabilità	Remote system answers to PING command
Livello rischio	Informazione
SPID	2853
Impatto	The remote system answers to the PING command. The PING command is u "Alive" on the Internet. By this an attacker can easily determine if the sy INTERNET and base other attacks on this.
Output della vulnerabilità / Evidenze	
	64 octets from 35.214.203.110: icmp_seq=0 ttl=117 time=53.8 ms