

TRACCIA S1 L2 ASSET ORGANIZZATIVI, MINACCE E VULNERABILITÀ

UN'AZIENDA VI HA INCARICATO DI SVOLGERE UN'ANALISI DELLE VULNERABILITÀ E DELLE MINACCE SUI PROPRI ASSET ORGANIZZATIVI. L'AZIENDA OPERA NEL SETTORE METALMECCANICO, PRODUZIONE DI INGRANAGGI, HA CIRCA 200 IMPIEGATI ED UN PROPRIO E-COMMERCE. SONO PRESENTI CIRCA 200 PC (1.000 €/PC) E 30 SERVER (3.000 €/SERVER). I SERVIZIO DI CUI DISPONE SONO: SITO E-COMMERCE (FATTURATO 10.000 €/GIORNO), ERP DI GESTIONE AZIENDALE (30.000€), SERVER DI POSTA ELETTRONICA (5.000€) E UN SISTEMA DI SICUREZZA COMPOSTO DA FIREWALL, IDS E SIEM DI (25.000€). NELLA GESTIONE DEL RISCHIO, L'IDENTIFICAZIONE DEGLI ASSET, L'ANALISI DELLE MINACCE E DELLE VULNERABILITÀ AVVIENE IN CONTEMPORANEA E SI INTEGRANO A VICENDA. CREARE UN REPORT IN CUI INCLUDERE:

1. IDENTIFICAZIONE E VALORE DEGLI ASSET
2. ANALISI DELLE VULNERABILITÀ
3. ANALISI DELLE MINACCE SIETE LIBERI DI ESTENDERE ED IPOTIZZARE LO SCENARIO, IL NUMERO DI ASSET DA CUI PARTIRE È A VOSTRA SCELTA. POTETE UTILIZZARE QUALSIASI SUPPORTO COME CVE, CVSS, TABELLE NIST SP 800-30, ECC.

1 ANALISI DELLE VULNERABILITÀ E DELLE MINACCE

Identificazione e Valore degli Asset

- PC: 200 unità, valore totale 200.000€ (1.000€ per PC)
- Server: 30 unità, valore totale 90.000€ (3.000€ per server)
- Sito e-commerce: Fatturato di 10.000€ al giorno
- ERP di gestione aziendale: Valore 30.000€
- Server di posta elettronica: Valore 5.000€
- Sistema di sicurezza (firewall, IDS, SIEM): Valore 25.000€

- **Common Vulnerabilities and Exposures (CVE):** Il CVE è un dizionario pubblico di vulnerabilità note in ambito informatico, gestito dal MITRE Corporation. Ogni vulnerabilità identificata riceve un identificatore unico in formato CVE-ANNO-NUMERO (es. CVE-2021-12345). Questo sistema permette di identificare e riferirsi in modo univoco alle vulnerabilità, facilitando la condivisione di informazioni e la collaborazione tra organizzazioni.
- **Common Vulnerability Scoring System(CVSS):** Il CVSS è uno standard aperto per valutare la gravità delle vulnerabilità informatiche. Assegna un punteggio numerico compreso tra 0 e 10, basato su metriche che considerano il vettore di attacco, l'impatto sulla riservatezza, l'integrità e la disponibilità, e altri fattori. È ampiamente utilizzato dalle organizzazioni e dai produttori di software per comunicare la gravità delle vulnerabilità e stabilire priorità di mitigazione. Queste sono due delle reportistiche e dizionari che utilizzeremo per catalogare e classificare le vulnerabilità presenti nelle slide successive

2. ANALISI DELLE VULNERABILITÀ

LE VULNERABILITÀ SONO STATE INDIVIDUATE NEI SEGUENTI ASSET PER L'ANALISI DELLE VULNERABILITÀ, SI POTREBBE FARE RIFERIMENTO A DATABASE DI VULNERABILITÀ COME IL COMMON VULNERABILITIES AND EXPOSURES (CVE) E UTILIZZARE IL COMMON VULNERABILITY SCORING SYSTEM (CVSS) PER VALUTARE LA GRAVITÀ DELLE VULNERABILITÀ IDENTIFICATE.

- Sito e-commerce:
- **CVE-2024-29184** : Vulnerabilità XSS che potrebbe permettere ad attaccanti di eseguire script malevoli sul browser dei clienti.

The screenshot displays the NIST CVE details page for CVE-2024-29184. At the top, there are tabs for 'Severity', 'CVSS Version 3.x', and 'CVSS Version 2.0'. The 'Severity' tab is active, showing 'CVSS 3.x Severity and Metrics:'. Below this, there are two main sections: 'NVD' and 'CNA'. The 'NVD' section shows 'NIST: NVD' and 'Base Score: N/A', with a note that 'NVD assessment not yet provided.' The 'CNA' section shows 'CNA: GitHub, Inc.' and 'Base Score: 8.0 HIGH'. A 'Vector' field displays 'CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H'. A detailed 'CVSS v3.1 Severity and Metrics' box is open, showing 'Base Score: 8.0 HIGH', 'Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H', 'Impact Score: 5.9', and 'Exploitability Score: 2.1'. Below this, a list of metrics is shown: 'Attack Vector (AV): Network', 'Attack Complexity (AC): Low', 'Privileges Required (PR): Low', 'User Interaction (UI): Required', 'Scope (S): Unchanged', 'Confidentiality (C): High', 'Integrity (I): High', and 'Availability (A): High'. At the bottom, there is a section for 'References to Advisories, Solutions, and Workarounds'.

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NVD NIST: NVD Base Score: N/A NVD assessment not yet provided.

CNA CNA: GitHub, Inc. Base Score: 8.0 HIGH Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

CVSS v3.1 Severity and Metrics:

Base Score: 8.0 HIGH
Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
Impact Score: 5.9
Exploitability Score: 2.1

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): Low
User Interaction (UI): Required
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

References to Advisories, Solutions, and Workarounds

By selecting these links, you will be leaving NIST webspace. We have provided these links because they may have information that would be of interest to you. No warranty is made by NIST for the accuracy of the information being referenced, or not, from this page. There may be other ways to find this information.

CVE-2024-24092: VULNERABILITÀ DI INJECTION CHE POTREBBE CONSENTIRE AD UN ATTACCANTE DI ESEGUIRE COMANDI NON AUTORIZZATI SUL SERVER.

CVE-2024-24092 Detail

AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.

Description

SQL Injection vulnerability in Code-projects.org Scholars Tracking System 1.0 allows attackers to run arbitrary code via login.php.

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: N/A

NVD assessment not yet provided.

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

QUICK INFO

CVE Dictionary Entry:

CVE-2024-24092

NVD Published Date:

03/12/2024

NVD Last Modified:

03/13/2024

Source:

MITRE

CVE-2024-0490: VULNERABILITÀ DI AUTENTICAZIONE DEBOLE CHE POTREBBE CONSENTIRE AD UN ATTACCANTE DI ACCEDERE INDEBITAMENTE AL SISTEMA ERP. MENTRE NELL'IMMAGINE È PRESENTE LA CLASSIFICA (CVSS)

processing of the file /user/getAllList. The manipulation leads to information disclosure. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.2 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-250595.

Source:
VulDB

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: 7.5 HIGH

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N



CNA: VulDB

Base Score: 5.3 MEDIUM

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

NVD Analysts use publicly available information to associate vector strings and CVSS information provided within the CVE List from the CNA.

Note: It is possible that the NVD CVSS may not match that of the CNA. The most common information does not provide sufficient detail or that information simply was not available was assigned.

CVSS v3.1 Severity and Metrics:

Base Score: 7.5 HIGH

Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Impact Score: 3.6

Exploitability Score: 3.9

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): None

User Interaction (UI): None

Scope (S): Unchanged

Confidentiality (C): High

Integrity (I): None

Availability (A): None

References to Advisories, Solutions, and Tools

CVE-2023-24932: VULNERABILITÀ DI SPOOFING DELL'INDIRIZZO EMAIL CHE POTREBBE ESSERE SFRUTTATA PER INVIARE EMAIL FRAUDOLENTE AI CLIENTI.


Description

Secure Boot Security Feature Bypass Vulnerability

Severity

CVSS Version 3.xCVSS Version 2.0

CVSS 3.x Severity and Metrics:

 **CNA:** Microsoft Corporation

Base Score: 6.7 MEDIUM

Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector string information provided within the CVE List from the CNA.

Note: The CNA providing a score has achieved an Acceptance Level of Provisional provided by this CNA.

References to Advisories, Solutions, and Workarounds

By selecting these links, you will be leaving NIST webspace. We have provided these links because they may have information that would be of interest to you. No information is being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose.

QUICK INFO

CVE Dictionary Entry:
CVE-2023-24932

NVD Published Date:
05/09/2023

NVD Last Modified:
05/15/2023

Source:
Microsoft Corporation

CVSS v3.1 Severity and Metrics:

Base Score: 6.7 MEDIUM

Vector: AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Impact Score: 5.9

Exploitability Score: 0.8

Attack Vector (AV): Local

Attack Complexity (AC): Low

Privileges Required (PR): High

User Interaction (UI): None

Scope (S): Unchanged

Confidentiality (C): High

Integrity (I): High

Availability (A): High

- Hardware:
- Mancanza di aggiornamenti regolari del software operativo sui PC e sui server, rendendo gli asset vulnerabili a exploit noti.

3. ANALISI DELLE MINACCE

SULLA BASE DELLE VULNERABILITÀ IDENTIFICATE, SONO STATE ANALIZZATE LE POSSIBILI MINACCE:

- Attacchi informatici:
- Attacchi di tipo XSS e Injection sul sito e-commerce per compromettere i dati dei clienti o rubare informazioni sensibili.
- Tentativi di accesso non autorizzato all'ERP aziendale per rubare informazioni finanziarie o sensibili dell'azienda.
- Utilizzo di email spoofing per ingannare i clienti e rubare informazioni personali o finanziarie.
- Perdita di dati:
- Rischio di perdita di dati sensibili dei clienti e dell'azienda a causa di violazioni della sicurezza informatica.
- Interruzione dei servizi:
- Possibilità di interruzione dei servizi critici come il sito e-commerce e l'ERP aziendale a causa di attacchi informatici o malfunzionamenti dei sistemi.

CONCLUSIONI

L'azienda deve affrontare urgentemente le vulnerabilità identificate per mitigare i rischi di attacchi informatici, perdita di dati e interruzione dei servizi. Si raccomanda di:

- Applicare patch e aggiornamenti regolari per correggere le vulnerabilità esistenti nei software e nei sistemi.
- Implementare misure di sicurezza aggiuntive come firewall avanzati e sistemi di rilevamento delle intrusioni per proteggere i sistemi critici.
- Condurre sessioni di formazione sulla sicurezza informatica per sensibilizzare il personale e ridurre il rischio di phishing e altre minacce basate sull'ingegneria sociale.
- Implementare politiche di accesso sicuro e autenticazione a due fattori per proteggere l'accesso ai sistemi critici.