Report di Valutazione delle Vulnerabilità

Data del Report: [24/10/2023]

Cliente: [Pippo]

Contatto: [Pippo]

Email: [pippo@pippo.net]

Telefono: [000000000000]

Introduzione:

Questo rapporto riporta i risultati della valutazione delle vulnerabilità condotta su [Windows XP-SP2] per conto del cliente [Pippo]. La valutazione delle vulnerabilità ha lo scopo di identificare e analizzare le possibili minacce alla sicurezza e le vulnerabilità dell'infrastruttura esaminata.

Risultati della Valutazione delle Vulnerabilità:

La valutazione delle vulnerabilità è stata effettuata attraverso una serie di strumenti e tecniche per identificare e classificare le vulnerabilità presenti nel sistema. Di seguito sono riportati i principali risultati:

2. **Vulnerabilità Rilevate**:

CVE-2008-1446: Integer overflow in the Internet Printing Protocol (IPP) ISAPI (Internet Printing Protocol) in Microsoft Internet Information Services (IIS) da 5.0 a 7.0 su Windows 2000 SP4, XP SP2 e SP3, Server 2003 SP1 e SP2 e Server 2008 consente agli utenti autenticati remoti di eseguire codice arbitrario tramite una richiesta HTTP POST che attiva una connessione IPP in uscita da un server Web a una macchina gestita dall'aggressore, nota anche come "Vulnerabilità del servizio IPP Overflow di numeri interi".

CVE-2005-4360: è una vulnerabilità ISS (Microsoft Internet Information Services) 5.1 su Windows XP Professional SP2 che consente agli aggressori remoti di eseguire codice arbitrario tramite più richieste a ".dll" seguite da argomenti come da "~0" a "~9", che causa ntdll .dll per produrre un valore restituito che non viene gestito correttamente da IIS, come dimostrato utilizzando "/_vti_bin/.dll/*/~0". NOTA: inizialmente si riteneva che la conseguenza fosse solo un rifiuto del servizio (crash e riavvio dell'applicazione).

CVE-2009-1535: L'estensione WebDAV in Microsoft Internet Information Services (IIS) 5.1 e 6.0. consente agli aggressori remoti di aggirare i meccanismi di protezione basati su URI ed elencare cartelle o leggere, creare o modificare file, tramite un %c0%af (Unicode/carattere) ad un livello posizione arbitraria nell'URI, come dimostrato inserendo %c0%af in un componente del nome percorso iniziale "/protected/" per bypassare la protezione con password sulla cartella protected\, ovvero "Vulnerabilità di bypass dell'autenticazione WebDAV di IIS 5.1 e 6.0".

CVE-2006-6578: vulnerabilità di Microsoft Internet Information Services (IIS) 5.1 che consente all'account IUSR_Machine di eseguire file non EXE come file .COM e che consente agli aggressori di eseguire comandi arbitrari tramite argomenti su qualsiasi file .COM che esegue tali argomenti, utilizzando win.com quando è in una directory web con determinate autorizzazioni.

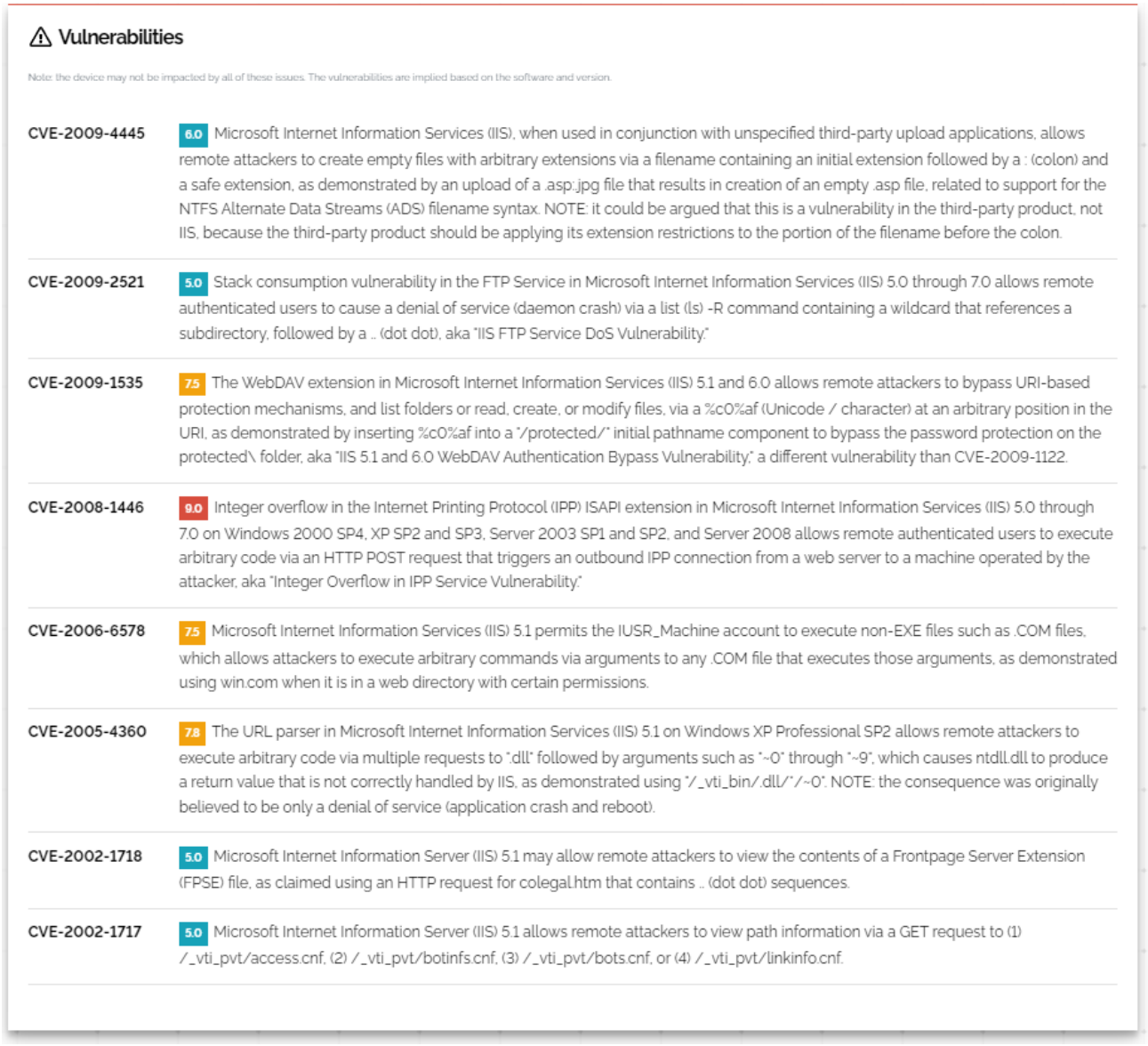
3. **Gravità delle Vulnerabilità valutata in punteggio**:

CVE-2008-1446: punteggio 9.0 > rischio Alto > sfruttabilità vulnerabilità 10

CVE-2005-4360: punteggio 7.8 > rischio Alto > sfruttabilità vulnerabilità 10

CVE-2009-1535: punteggio 7.5 > rischio Alto > sfruttabilità vulnerabilità 10

CVE-2006-6578: punteggio 7.5 > rischio Alto > sfruttabilità vulnerabilità 10



⚠ Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2009-4445	6.0 Microsoft Internet Information Services (IIS), when used in conjunction with unspecified third-party upload applications, allows remote attackers to create empty files with arbitrary extensions via a filename containing an initial extension followed by a : (colon) and a safe extension, as demonstrated by an upload of a .asp:.jpg file that results in creation of an empty .asp file, related to support for the NTFS Alternate Data Streams (ADS) filename syntax. NOTE: it could be argued that this is a vulnerability in the third-party product, not IIS, because the third-party product should be applying its extension restrictions to the portion of the filename before the colon.
CVE-2009-2521	5.0 Stack consumption vulnerability in the FTP Service in Microsoft Internet Information Services (IIS) 5.0 through 7.0 allows remote authenticated users to cause a denial of service (daemon crash) via a list (ls) -R command containing a wildcard that references a subdirectory, followed by a .. (dot dot), aka "IIS FTP Service DoS Vulnerability."
CVE-2009-1535	7.5 The WebDAV extension in Microsoft Internet Information Services (IIS) 5.1 and 6.0 allows remote attackers to bypass URI-based protection mechanisms, and list folders or read, create, or modify files, via a %c0%af (Unicode / character) at an arbitrary position in the URI, as demonstrated by inserting %c0%af into a "/protected/" initial pathname component to bypass the password protection on the protected\ folder, aka "IIS 5.1 and 6.0 WebDAV Authentication Bypass Vulnerability," a different vulnerability than CVE-2009-1122.
CVE-2008-1446	9.0 Integer overflow in the Internet Printing Protocol (IPP) ISAPI extension in Microsoft Internet Information Services (IIS) 5.0 through 7.0 on Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, and Server 2008 allows remote authenticated users to execute arbitrary code via an HTTP POST request that triggers an outbound IPP connection from a web server to a machine operated by the attacker, aka "Integer Overflow in IPP Service Vulnerability."
CVE-2006-6578	7.5 Microsoft Internet Information Services (IIS) 5.1 permits the IUSR_Machine account to execute non-EXE files such as .COM files, which allows attackers to execute arbitrary commands via arguments to any .COM file that executes those arguments, as demonstrated using win.com when it is in a web directory with certain permissions.
CVE-2005-4360	7.8 The URL parser in Microsoft Internet Information Services (IIS) 5.1 on Windows XP Professional SP2 allows remote attackers to execute arbitrary code via multiple requests to ".dll" followed by arguments such as "~0" through "~9", which causes ntdll.dll to produce a return value that is not correctly handled by IIS, as demonstrated using "/_vti_bin/.dll/"/~0". NOTE: the consequence was originally believed to be only a denial of service (application crash and reboot).
CVE-2002-1718	5.0 Microsoft Internet Information Server (IIS) 5.1 may allow remote attackers to view the contents of a Frontpage Server Extension (FPSE) file, as claimed using an HTTP request for colegal.htm that contains .. (dot dot) sequences.
CVE-2002-1717	5.0 Microsoft Internet Information Server (IIS) 5.1 allows remote attackers to view path information via a GET request to (1) /_vti_pvt/access.cnf, (2) /_vti_pvt/botinfs.cnf, (3) /_vti_pvt/bots.cnf, or (4) /_vti_pvt/linkinfo.cnf.

4. **Raccomandazion**i:

- Verificare se è disponibile un aggiornamento o una patch disponibile e fornita dal fornitore del software o del sistema che risolvono la vulnerabilità e applicare le correzioni il prima possibile.
- Nel caso in cui non sia possibile applicare una patch immediata, isolare o limitare l'accesso alla parte vulnerabile dell'infrastruttura per ridurre il rischio di sfruttamento.
- Mantenere un monitoraggio costante della situazione, che includere il monitoraggio dei registri, l'analisi del traffico di rete o l'uso di sistemi di rilevamento delle intrusioni per individuare eventuali tentativi di sfruttamento della vulnerabilità.
- Assicurarsi che il personale sia consapevole della vulnerabilità e delle contromisure da adottare in quanto l'educazione sulla sicurezza è fondamentale.
- Eseguire regolari backup dei dati critici in modo che, in caso di compromissione i dati possono essere ripristinati.
- Assicurarsi sempre di seguire le linee guida fornite dai fornitori e dalle autorità competenti.

Conclusione:

La valutazione delle vulnerabilità ha rilevato una serie di possibili minacce alla sicurezza che richiedono l'attenzione del cliente. È fondamentale prendere in considerazione le raccomandazioni fornite e implementare le azioni correttive necessarie per migliorare la sicurezza dell'infrastruttura.

Analisi vulnerabilità sito web

Introduzione:

Questo rapporto riporta i risultati della valutazione delle vulnerabilità condotta sul sito web aziendale per conto del cliente [Pippo]. La valutazione delle vulnerabilità ha lo scopo di identificare e analizzare le possibili minacce alla sicurezza e le vulnerabilità della risorsa, più precisamente sull'headers

Risultati della Valutazione delle Vulnerabilità.

La valutazione delle vulnerabilità è stata effettuata attraverso una serie di strumenti e tecniche per identificare e classificare le vulnerabilità presenti nel sistema. Di seguito sono riportati i principali risultati:

Vulnerabilità di Oracle MySQL Server <= 5.7.33 / 8.0 <= 8.0.23 Security Update (cpuapr2021) – Windows ed è legato a problemi di sicurezza che possono essere sfruttati da attaccanti per compromettere o mettere a rischio l'integrità, la riservatezza o la disponibilità dei dati memorizzati in un database MySQL

Raccomandazione:

eseguire l'aggiornamento alla nuova versione della Oracle.

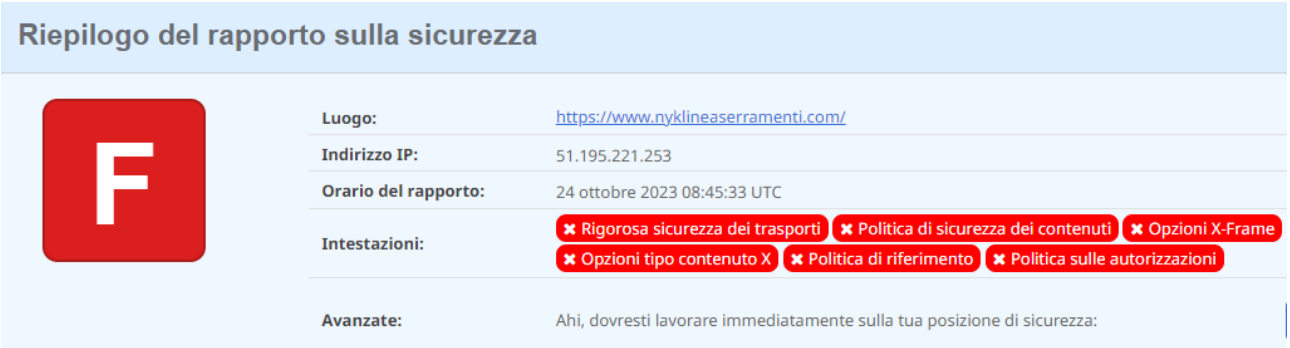
Configurare le autorizzazioni di accesso in modo rigoroso, assegnando solo i privilegi necessari agli utenti e ai ruoli.

Usare password robuste e limitare l'accesso ai comandi SQL e alle funzionalità solo ai contesti appropriati.

Validare e sanificare sempre i dati in ingresso per prevenire le injection attacks.

Monitorare costantemente il sistema per rilevare attività sospette.

Eseguire backup regolari dei dati del database.



Strict-Transport-Security: è un meccanismo di sicurezza progettato per migliorare la sicurezza delle comunicazioni web impedendo il downgrade a HTTP da HTTPS e, quindi, proteggendo gli utenti da attacchi di tipo Man-in-the-Middle. è un'eccellente funzionalità da supportare sul tuo sito e rafforza l'implementazione di TLS facendo sì che l'agente utente imponga l'uso di HTTPS.

Opzioni X-Frame: sono intestazioni HTTP che vengono utilizzate per controllare il comportamento dei browser web in relazione all'embedding di contenuti web in un frame o iframe all'interno di un'altra pagina web. Queste intestazioni forniscono un meccanismo di sicurezza per mitigare i rischi legati a attacchi di tipo clickjacking o altre forme di framing malevolo.

X-Content-Type-Options: durante il controllo è stato rilevata la vulnerabilità di attacchi MIME (Multipurpose Internet Mail Extensions) nello specifico MIME-sniffing o content sniffing. Questi tipi di attacco possono interpretare erroneamente i tipi di contenuto dei file scaricati.

Content Security Policy - An Introduction: la scansione ha rilevato una vulnerabilità esposta ad attacchi XSS (Cross Site Scripting) una categoria di vulnerabilità informatiche che consentono a un attaccante di iniettare script malevoli in javascript, compiendo il furto di cookie di sessione, il reindirizzamento degli utenti su pagine malevole, la diffusione di malware, la visualizzazione di contenuti dannosi o il danneggiamento del sito web stesso.

Referrer Policy: è un controllo più preciso della privacy e sulla sicurezza rispetto all'intestazione HTTP "Referer" predefinita, il rapporto fornisce che la pagina di destinazione può conoscere la pagina da cui l'utente proviene, e talvolta questo può essere indesiderato o rappresentare un rischio per la privacy.

Permissions Policy: meccanismi di sicurezza web che consentono ai proprietari di siti web di definire in modo granulare quali risorse e funzionalità un'applicazione web può accedere e utilizzare, la scansione individua tale vulnerabilità che comprende l'accesso a telecamere, microfoni, geolocalizzazione, accesso a cookie di terze parti e altro.

Raccomandazioni:

Per Opzioni X-Frame che è stato gradualmente sostituito da un nuovo meccanismo noto come Content Security Policy (CSP), offre un controllo più ampio sulla sicurezza della pagina web, inclusi gli iframe e il framing. Tuttavia, le X-Frame-Options possono ancora essere utili per aggiungere un ulteriore strato di sicurezza, in particolare su siti legacy o in combinazione con altre misure di sicurezza.

Per il X-Content-Type-Options Includere questa intestazione nelle risposte HTTP è una pratica consigliata per migliorare la sicurezza delle tue applicazioni web. Previeni il content sniffing, che potrebbe essere utilizzato da un attaccante per cercare di ingannare il browser e gli utenti finali sul tipo di contenuto dei file scaricati, contribuendo così a ridurre i rischi di vulnerabilità legati alla sicurezza.

Per le Referrer policy, la scelta dell'opzione appropriata dipende dalle esigenze di privacy e sicurezza del sito web. La Referrer Policy è uno strumento importante per aiutare a mitigare potenziali rischi legati alla privacy, come il rivelamento involontario di informazioni sensibili nell'URL di riferimento.

Per prevenire gli attacchi XSS, è fondamentale adottare pratiche di sviluppo sicuro, inclusa la validazione e la sanificazione dei dati in ingresso, l'uso di contesti di codifica appropriati e l'implementazione di meccanismi di sicurezza come i Content Security Policy (CSP) per limitare l'esecuzione di script non autorizzati. Gli sviluppatori e gli amministratori dei siti web devono essere consapevoli di queste minacce e adottare misure per proteggere le applicazioni e gli utenti.

Le Permissions Policy possono essere configurate nel codice del sito web o tramite il server HTTP per influenzare il comportamento del browser.

Giovanni Saponaro