Vulnerability Assessment con Nessus su Metasploitable

Introduzione

In questo esercizio, abbiamo utilizzato Nessus per effettuare una valutazione delle vulnerabilità sulla macchina Metasploitable. L'obiettivo era identificare e analizzare le vulnerabilità presenti.

Analisi del Report

Vulnerabilità: 70728 - Apache PHP-CGI Remote Code Execution

Synopsis

Il server web remoto contiene una versione di PHP che permette l'esecuzione di codice arbitrario.

Descrizione

L'installazione di PHP sul server web remoto contiene un difetto che potrebbe permettere a un attaccante remoto di passare argomenti della linea di comando come parte di una stringa di query al programma PHP-CGI. Questo potrebbe essere sfruttato per eseguire codice arbitrario, rivelare il codice sorgente di PHP, causare un crash del sistema, ecc.

Soluzione

Aggiornare PHP alla versione 5.3.13, 5.4.3 o successiva.

Dettagli di Rischio

Fattore di Rischio: Alto
CVSS v3.0 Base Score: 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSS v3.0 Temporal Score: 9.4 (CVSS:3.0/E:H/RL:O/RC:C)
VPR Score: 9.2
CVSS v2.0 Base Score: 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS v2.0 Temporal Score: 6.5 (CVSS2#E:H/RL:OF/RC:C)

Riferimenti

BID: 53388
CVE:
- CVE-2012-1823
- CVE-2012-2311
- CVE-2012-2336

- CVE-2012-2337
- CVE-2012-2338

Approfondimento

Apache PHP-CGI Remote Code Execution

La vulnerabilità risiede nel modo in cui il PHP-CGI gestisce gli argomenti della linea di comando quando sono passati come parte di una stringa di query. Questo difetto può essere sfruttato da un attaccante remoto per eseguire comandi arbitrari con i permessi del processo PHP, causando potenzialmente un grande danno al sistema. Questo tipo di vulnerabilità è particolarmente critico su server web pubblicamente accessibili, poiché potrebbe permettere a un attaccante di prendere il controllo completo del server.

Impatto

Confidenzialità: Alta - L'attaccante potrebbe accedere a dati sensibili.
Integrità: Alta - L'attaccante potrebbe modificare i contenuti del server.
Disponibilità: Alta - L'attaccante potrebbe causare un crash del sistema.

Raccomandazioni

È fondamentale aggiornare PHP alla versione 5.3.13, 5.4.3 o successiva il più presto possibile. Gli aggiornamenti includono correzioni per queste vulnerabilità e miglioramenti nella gestione degli argomenti della linea di comando, prevenendo l'esecuzione di codice non autorizzato.

Vulnerabilità: 134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis

C'è un connettore AJP vulnerabile in ascolto sull'host remoto.

Descrizione

È stata trovata una vulnerabilità di inclusione/lettura file nel connettore AJP. Un attaccante remoto non autenticato potrebbe sfruttare questa vulnerabilità per leggere file di applicazioni web da un server vulnerabile. Nei casi in cui il server vulnerabile permetta il caricamento di file, un attaccante potrebbe caricare codice JavaServer Pages (JSP) malevolo all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

Soluzione

Aggiornare la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat alla versione 7.0.100, 8.5.51, 9.0.31 o successiva.

Dettagli di Rischio

Fattore di Rischio: Alto
CVSS v3.0 Base Score: 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSS v3.0 Temporal Score: 9.4 (CVSS:3.0/E:H/RL:O/RC:C)
VPR Score: 9.2
CVSS v2.0 Base Score: 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS v2.0 Temporal Score: 6.5 (CVSS2#E:H/RL:OF/RC:C)

Riferimenti

CVE:
- CVE-2020-1745
- CVE-2020-1938
- CISA-KNOWN-EXPLOITED-2022/03/17
- CEA-ID-CEA-2020-0021

Approfondimento

Apache Tomcat AJP Connector Request Injection (Ghostcat)

La vulnerabilità risiede nel modo in cui il connettore AJP gestisce le richieste. Un attaccante remoto può sfruttare questa vulnerabilità per leggere file dalle applicazioni web o, in scenari peggiori, eseguire codice arbitrario caricando file JSP malevoli. Questa vulnerabilità è particolarmente critica nei server che permettono il caricamento di file da utenti non autenticati, poiché può portare all'esecuzione di codice remoto e al controllo completo del server.

Impatto

Confidenzialità: Alta - L'attaccante potrebbe accedere a dati sensibili.
Integrità: Alta - L'attaccante potrebbe modificare i contenuti del server.
Disponibilità: Alta - L'attaccante potrebbe causare un crash del sistema.

Raccomandazioni

È fondamentale aggiornare la configurazione AJP per richiedere l'autorizzazione e aggiornare il server Tomcat alle versioni 7.0.100, 8.5.51, 9.0.31 o successiva il più presto possibile. Gli aggiornamenti includono correzioni per queste vulnerabilità e miglioramenti nella gestione delle richieste, prevenendo l'esecuzione di codice non autorizzato.

Vulnerabilità: 171340 - Apache Tomcat EoL (<= 5.5.x)

Synopsis

È installata una versione non supportata di Apache Tomcat sull'host remoto.

Descrizione

Secondo la versione, Apache Tomcat è inferiore o uguale alla versione 5.5.x. Pertanto, non è più mantenuto dal suo fornitore o provider. La mancanza di supporto implica che non verranno rilasciate nuove patch di sicurezza per il prodotto. Di conseguenza, potrebbe contenere vulnerabilità di sicurezza.

Soluzione

Aggiornare ad una versione di Apache Tomcat attualmente supportata.

Dettagli di Rischio

Fattore di Rischio: Critico

CVSS v3.0 Base Score: 10.0 (CVSS:3.0/AV

CVSS v2.0 Base Score: 10.0 (CVSS2#AV

Riferimenti

https://tomcat.apache.org/tomcat-55-eol.html

Approfondimento

La vulnerabilità riguarda l'utilizzo di una versione obsoleta di Apache Tomcat che non riceve più aggiornamenti di sicurezza. Questo comporta un rischio significativo poiché le vulnerabilità scoperte dopo la fine del supporto (EoL) non vengono risolte, esponendo il sistema a potenziali attacchi. L'aggiornamento a una versione supportata di Apache Tomcat è essenziale per garantire la sicurezza del server e mitigare i rischi associati a questa vulnerabilità.

Impatto

Confidenzialità: Alta - L'attaccante potrebbe accedere a dati sensibili.

Integrità: Alta - L'attaccante potrebbe modificare i contenuti del server.

Disponibilità: Alta - L'attaccante potrebbe causare un crash del sistema.

Raccomandazioni

È fondamentale aggiornare Apache Tomcat a una versione attualmente supportata il più presto possibile. Gli aggiornamenti includono correzioni per vulnerabilità conosciute e miglioramenti nella sicurezza, prevenendo l'esecuzione di codice non autorizzato e altri attacchi.

Vulnerabilità: 51988 - Bind Shell Backdoor Detection

Synopsis

L'host remoto potrebbe essere stato compromesso.

Descrizione

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un attaccante potrebbe utilizzarla connettendosi alla porta remota e inviando comandi direttamente.

Soluzione

Verificare se l'host remoto è stato compromesso e reinstallare il sistema se necessario.

Dettagli di Rischio

Fattore di Rischio: Critico

CVSS v3.0 Base Score: 9.8 (CVSS:3.0/AV

CVSS v2.0 Base Score: 10.0 (CVSS2#AV

Plugin Output

Nessus was able to execute the command 'id' using the following request:

tcp/1524/wild_shell

Approfondimento

La vulnerabilità riguarda la presenza di una shell bind sul sistema remoto che ascolta su una porta senza richiedere autenticazione. Questa situazione rappresenta un grave rischio di sicurezza poiché permette a un attaccante di prendere il controllo del sistema inviando comandi direttamente alla shell. È essenziale verificare immediatamente l'integrità del sistema e procedere con una reinstallazione se necessario per rimuovere eventuali backdoor e ripristinare la sicurezza del sistema.

Impatto

Confidenzialità: Alta - L'attaccante potrebbe accedere a dati sensibili.

Integrità: Alta - L'attaccante potrebbe modificare i contenuti del server.

Disponibilità: Alta - L'attaccante potrebbe causare un crash del sistema.

Raccomandazioni

È fondamentale verificare se l'host remoto è stato compromesso. Se risulta compromesso, è necessario reinstallare il sistema per rimuovere eventuali backdoor e ripristinare la sicurezza. Inoltre, si consiglia di implementare misure di sicurezza aggiuntive per prevenire future compromissioni.

Conclusione generale

L'esercizio ha permesso di familiarizzare con Nessus e con alcune vulnerabilità comuni. Questo tipo di valutazione è cruciale per mantenere sicuri i sistemi e identificare potenziali punti deboli.