Utilizzo di Cisco Secure IDS/NetRanger Custom String Match Signatures per "Code Red" Worm Remote Buffer Overflow in Microsoft Index Server ISAPI Extension in IIS 4.0 e 5.0

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Convenzioni
Firme stringa personalizzata
Firma 1: accesso al server di indice con tentativo di sfruttamento
Firma 2 — Worm "Code Red" di overflow del buffer di accesso al server di indice
Informazioni correlate

Introduzione

Alla fine di luglio 2003, Computer Economics (un'organizzazione di ricerca indipendente a Carlsbad, California) ha stimato che il worm "Code Red" era costato alle aziende 1,2 miliardi di dollari (USA) in termini di recupero dai danni alla rete e di perdita di produttività. Questa stima è aumentata in modo significativo con la successiva uscita del più potente verme "Code Red II". Cisco Secure Intrusion Detection System (IDS), un componente chiave del Cisco SAFE Blueprint, ha dimostrato il proprio valore nel rilevare e ridurre i rischi per la sicurezza della rete, tra cui il worm "Code Red".

Questo documento descrive un aggiornamento software per rilevare il metodo di utilizzo utilizzato dal worm "Code Red" (vedere la firma 2 di seguito).

È possibile creare le firme personalizzate di corrispondenza tra stringhe illustrate di seguito per rilevare lo sfruttamento di un overflow del buffer per i server Web che eseguono Microsoft Windows NT e Internet Information Services (IIS) 4.0 o Windows 2000 e IIS 5.0. Si noti inoltre che anche il servizio di indicizzazione in Windows XP beta è vulnerabile. L'advisory della sicurezza che descrive questa vulnerabilità è disponibile all'indirizzo http://www.eeye.com/html/Research/Advisories/AD20010618.html. Microsoft ha rilasciato una patch per questa vulnerabilità che può essere scaricata da http://www.microsoft.com/technet/security/bulletin/MS01-033.mspx.

Le firme discusse in questo documento sono disponibili nella versione di aggiornamento della firma S(5). Cisco Systems consiglia di aggiornare i sensori alla versione 2.2.1.8 o 2.5(1)S3 prima

di implementare questa firma. Gli utenti registrati possono scaricare questi aggiornamenti delle firme da Cisco Secure Software Center. Tutti gli utenti possono contattare il supporto tecnico Cisco tramite e-mail e telefono tramite i contatti Cisco internazionali.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Microsoft Windows NT e IIS 4.0
- Microsoft Windows 2000 e IIS 5.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Firme stringa personalizzata

Per risolvere questo problema, sono disponibili due firme personalizzate specifiche per le corrispondenze tra stringhe. Di seguito viene fornita una descrizione di ogni firma e vengono fornite le impostazioni del prodotto applicabili.

Firma 1: accesso al server di indice con tentativo di sfruttamento

Questa firma viene attivata in seguito a un tentativo di overflow del buffer nell'estensione ISAPI del server di indicizzazione, in combinazione con un tentativo di passare il codice della shell al server per ottenere l'accesso privilegiato nella forma originale del codice. La firma viene attivata solo nel tentativo di passare il codice della shell al servizio di destinazione nel tentativo di ottenere l'accesso completo a livello di sistema. Uno dei possibili problemi è che questa firma non viene attivata se l'autore dell'attacco non tenta di passare alcun codice shell, ma esegue l'overflow del buffer sul servizio nel tentativo di arrestare IIS e creare una negazione del servizio.

Stringa

```
[Gg][Ee][Tt].*[.][Ii][Dd][Aa][\x00-\x7f]+[\x80-\xff]
```

Impostazioni prodotto

- Occorrenze: 1
- Porta: 80

Nota: se si dispone di server Web in ascolto su altre porte TCP (ad esempio, 8080), è necessario creare una stringa personalizzata separata per ciascun numero di porta.

- Livello di gravità consigliato per l'allarme:
  - Alto (Cisco Secure Policy Manager)
  - 5 (Director Unix)
- Direzione:

  A

Firma 2 — Worm "Code Red" di overflow del buffer di accesso al server di indice

La seconda firma viene attivata in seguito a un tentativo di overflow del buffer sull'estensione ISAPI del server di indicizzazione, in combinazione con un tentativo di passare il codice della shell al server per ottenere l'accesso privilegiato nella forma offuscata utilizzata dal worm "Code Red". Questa firma viene attivata solo nel tentativo di passare il codice della shell al servizio di destinazione nel tentativo di ottenere l'accesso completo a livello di sistema. Uno dei possibili problemi è che questa firma non viene attivata se l'autore dell'attacco non tenta di passare alcun codice shell, ma esegue l'overflow del buffer sul servizio nel tentativo di arrestare IIS e creare una negazione del servizio.

Stringa

```
[/]default[.]ida[?][a-zA-Z0-9]+%u
```

Nota: nella stringa sopra riportata non sono presenti spazi vuoti.

Impostazioni prodotto

- Occorrenze: 1
- Porta: 80

Nota: se si dispone di server Web in ascolto su altre porte TCP (ad esempio, 8080), è necessario

creare una stringa personalizzata separata per ciascun numero di porta.

- Livello di gravità consigliato per l'allarme:
  - Alto (Cisco Secure Policy Manager)
  - 5 (Director Unix)
- Direzione:

  A

Per ulteriori informazioni su Cisco Secure IDS, fare riferimento a Cisco Secure Intrusion Detection.

Informazioni correlate

- Supporto tecnico - Router
- Consulenze sulla sicurezza Cisco
- Pagina di supporto per Cisco Secure Intrusion Detection
- Supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).