Computer Emergency Response Team

BOLLETTINO IT-CERT.180207.B01

Vulnerabilità in GNU C Library (glibc) (CVE-2018-6485)

MINISTERO DELLO
SVILUPPO ECONOMICO

DESCRIZIONE

La GNU C Library (**glibc**) è la libreria standard del linguaggio di programmazione C del progetto GNU. Questa libreria è inclusa in tutte le moderne distribuzioni di Linux in quanto fornisce l'interfaccia alle applicazioni che girano nello spazio utente (*shell* e altre utility) per effettuare chiamate di sistema e accedere alle altre strutture di base definite nel *kernel* di Linux.

È stata scoperta una vulnerabilità in glibc che potrebbe consentire l'esecuzione di codice arbitrario da remoto. In particolare, la vulnerabilità è legata ad una condizione di tipo *integer overflow* nella funzione `posix_memalign()` che si verifica quando le funzioni interne `memalign()` e `malloc()` non riportano correttamente errori nell'allocazione della memoria.

Un attaccante potrebbe tentare di sfruttare questa vulnerabilità inviando dati opportunamente predisposti ad un sistema affetto. Lo sfruttamento di questa vulnerabilità potrebbe consentire all'attaccante di ottenere gli stessi privilegi dell'applicazione affetta. A seconda dei privilegi associati all'applicazione sfruttata, l'attaccante potrebbe essere in grado di installare programmi, visualizzare, modificare o eliminare dati o creare nuovi *account* con diritti utente completi. Tentativi falliti di sfruttare questa vulnerabilità potrebbero portare al *crash* dell'applicazione con conseguente condizione di *denial of service*.

Al momento non ci sono notizie che questa vulnerabilità sia stata sfruttata in attacchi reali.

Sono disponibili aggiornamenti software che risolvono la vulnerabilità nei prodotti interessati (per maggiori informazioni si veda la sezione LINK UTILI).

SOLUZIONE

La vulnerabilità oggetto del presente bollettino è stata risolta nella versione 2.27 del pacchetto glibc.

Si raccomanda ai gestori di sistemi basati su Linux di verificare la disponibilità di una *patch* per il pacchetto glibc per la propria distribuzione e, nel caso, di eseguire l'aggiornamento.

SISTEMI

GNU glibc versione 2.26 e precedenti.

La GNU C Library è inclusa nelle seguenti distribuzioni Linux (lista non esaustiva):

- Caldera OpenLinux Server
- Caldera OpenLinux Workstation
- Debian Linux
- EnGarde Secure Linux
- Gentoo Linux
- HP Secure OS software for Linux
- MandrakeSoft Corporate Server
- Mandriva Linux Mandrake
- Openwall GNU/*/Linux

- Red Hat Enterprise Linux
- Red Hat Linux
- Red Hat Linux Advanced Work Station
- Slackware Linux
- Sun Linux
- SuSE Linux
- SuSE Linux Enterprise Server
- Ubuntu Linux
- Trustix Secure Linux
- Wirex Immunix OS

LINK UTILI

The GNU C Library (glibc)

https://www.gnu.org/software/libc/

Sourceware

https://sourceware.org/bugzilla/show_bug.cgi?id=22343
https://sourceware.org/glibc/wiki/Release/2.27

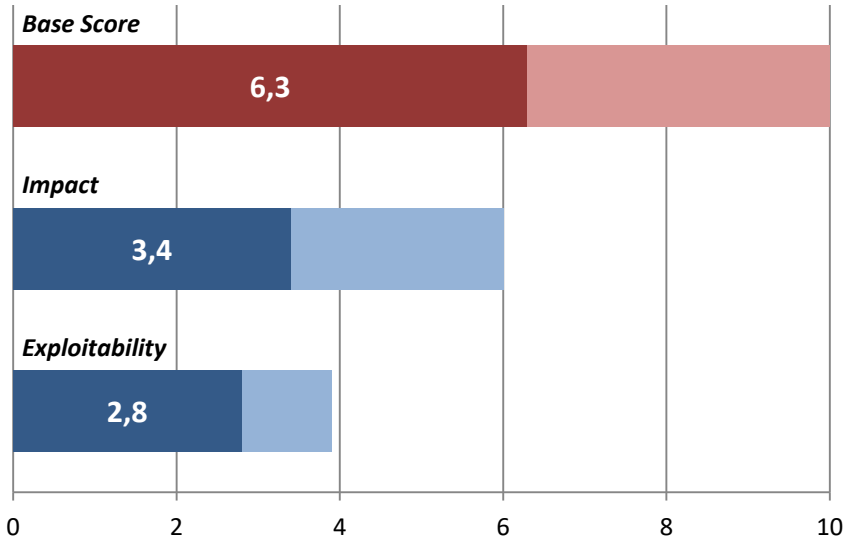
Avvisi dei produttori

https://access.redhat.com/security/cve/cve-2018-6485
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=878159
https://bugs.gentoo.org/show_bug.cgi?id=CVE-2018-6485
https://people.canonical.com/~ubuntu-security/cve/2018/CVE-2018-6485.html

Mitre CVE ID

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6485

VALUTAZIONE CVSS



Relativamente alla valutazione della *severity* come metrica di base - da intendersi quale livello di pericolosità della vulnerabilità delle componenti di sistema o delle piattaforme - il CERT Nazionale valuta i parametri che concorrono al calcolo della *Base Score* secondo lo standard CVSS v3 (*Common Vulnerabilities Scoring System*), avvalendosi del *tool* messo a disposizione dal sito del NIST (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator).

Nello specifico, sulla base di informazioni preliminari soggette ad aggiornamento, sono stati raggiunti i seguenti punteggi:

- *Base Score:* 6,3
- *Impact:* 3,4
- *Exploitability:* 2,8

Vettore CVSS: AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

NOTE

Le informazioni contenute nel presente bollettino sono fornite a meri fini informativi.

In nessun caso il CERT Nazionale può essere ritenuto responsabile di qualunque perdita, pregiudizio, responsabilità, costo, onere o spesa, ivi comprese le eventuali spese legali, danno diretto, indiretto, incidentale o consequenziale, derivante da o connesso alle informazioni riportate nel presente bollettino.

La versione PDF del bollettino è statica ed, in quanto tale, contiene le informazioni disponibili al momento della pubblicazione.