Computer Emergency Response Team

BOLLETTINO IT-CERT.180521.B01

Vulnerabilità multiple in ISC BIND

(CVE-2018-5736, CVE-2018-5737)

MINISTERO DELLO
SVILUPPO ECONOMICO

DESCRIZIONE

BIND è un software open source sviluppato da ISC (*Internet Systems Consortium*) che implementa i protocolli di *Domain Name System* (DNS) di Internet. Si tratta di una implementazione di riferimento di tali protocolli, ma è anche un software largamente utilizzato su sistemi in produzione, adatto per l'uso in applicazioni ad alta capacità ed alta affidabilità. Il nome BIND sta per "Berkeley Internet Name Domain", in quanto il software è nato nei primi anni 80 presso l'Università della California a Berkeley.

Sono state riscontrate due vulnerabilità di media gravità in ISC BIND 9 che, se sfruttate con successo da un attaccante remoto, possono causare la terminazione del componente DNS server `named` o altri comportamenti anomali, con conseguente condizione di *denial of service* o di degrado del servizio.

Si riportano per informazione brevi descrizioni delle vulnerabilità (in Inglese) con i rispettivi codici CVE:

- **CVE-2018-5736**: Multiple transfers of a zone in quick succession can cause an assertion failure in `rbtdb.c`
- **CVE-2018-5737**: BIND 9.12's serve-stale implementation can cause an assertion failure in `rbtdb.c` or other undesirable behavior, even if serve-stale is not enabled.

Al momento non ci sono notizie che queste vulnerabilità siano state sfruttate in attacchi reali.

È disponibile un aggiornamento che risolve queste vulnerabilità in ISC BIND. È altresì disponibile una soluzione alternativa per mitigare la vulnerabilità CVE-2018-5737 (per maggiori informazioni si veda la sezione LINK UTILI).

SOLUZIONE

Aggiornare ISC BIND alla versione 9.12.1-P2.

In attesa di applicare l'aggiornamento, come soluzione alternativa di mitigazione per la sola vulnerabilità CVE-2018-5737 è possibile impostare l'opzione "max-stale-ttl 0;" in `named.conf` (per maggiori informazioni si veda la sezione LINK UTILI).

SISTEMI

Risultano affette dalle vulnerabilità descritte in questo bollettino le seguenti versioni di ISC BIND:

- BIND versione 9.12.0
- BIND versione 9.12.1

LINK UTILI

Download BIND

http://www.isc.org/downloads/

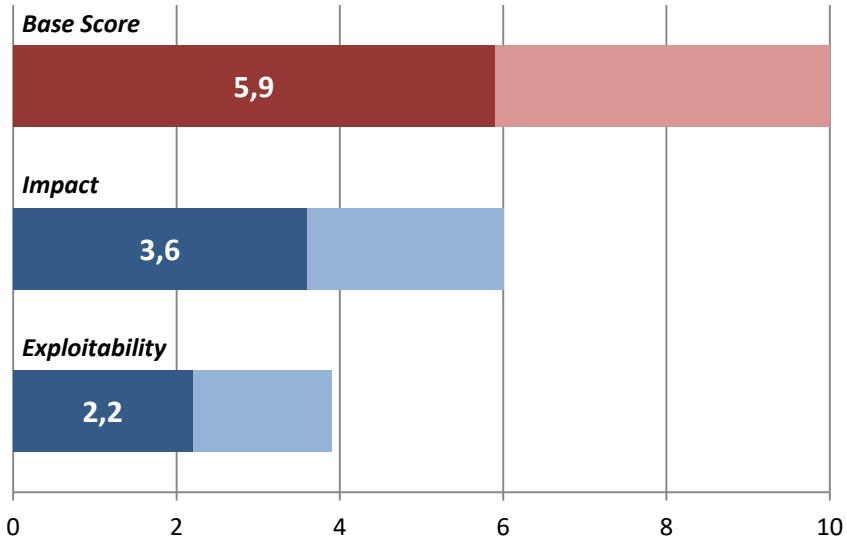
ISC BIND Security Advisory

https://kb.isc.org/article/AA-01602
https://kb.isc.org/article/AA-01606

Mitre CVE ID

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5736
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5737

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, per la sola vulnerabilità **CVE-2018-5737**, sono stati raggiunti i seguenti punteggi:

- *Base Score:* 5,9
- *Impact:* 3,6
- *Exploitability:* 2,2

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

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.