Computer Emergency Response Team

BOLLETTINO IT-CERT.200204.B01

Vulnerabilità critica in OpenSMTPD (CVE-2020-7247)

MINISTERO DELLO
SVILUPPO ECONOMICO

DESCRIZIONE

OpenSMTPD è un'implementazione *open source* del protocollo SMTP (*Simple Mail Transfer Protocol*) utilizzato come mail server in **OpenBSD** ed in altri prodotti software.

È stata scoperta una vulnerabilità critica (CVE-2020-7247) in OpenSMTPD che può consentire ad un attaccante locale o remoto di elevare i propri privilegi ed eseguire codice arbitrario.

La vulnerabilità è legata ad una validazione impropria degli indirizzi Email di origine e di destinazione nella funzione `smtp_mailaddr()`. Nel caso in cui la porzione di un indirizzo che precede il simbolo `@` (local-part) non risulta valida e il nome di dominio è vuoto, la funzione vulnerabile non restituisce un errore come previsto ma aggiunge il nome di dominio predefinito all'indirizzo.

La vulnerabilità può essere sfruttata mediante l'invio di messaggi SMTP appositamente predisposti, contenenti caratteri speciali non consentiti e potenzialmente pericolosi nella parte locale dell'indirizzo di provenienza. Se sfruttata con successo, questa vulnerabilità può consentire all'attaccante di aggirare la validazione degli indirizzi e di eseguire comandi di *shell* arbitrari con i privilegi di *root*.

OpenBSD ha rilasciato un aggiornamento che risolve la vulnerabilità nelle versioni affette di OpenSMTPD (per maggiori informazioni si veda la sezione LINK UTILI).

SOLUZIONE

Per risolvere la vulnerabilità oggetto di questo bollettino è necessario aggiornare OpenSMTPD alla versione 6.6.1p1.

Per maggiori informazioni sulla vulnerabilità, sui prodotti vulnerabili e sugli aggiornamenti disponibili, si raccomanda di consultare la documentazione online elencata nella sezione LINK UTILI.

SISTEMI

Risulta affetta dalla vulnerabilità descritta in questo bollettino la versione 6.6 di OpenSMTPD, utilizzata in OpenBSD 6.6 e in altri prodotti software, tra cui diverse distribuzioni Linux

LINK UTILI

Qualys Security Advisory

https://www.qualys.com/2020/01/28/cve-2020-7247/lpe-rce-opensmtpd.txt

OpenSMTPD releases

https://github.com/OpenSMTPD/OpenSMTPD/releases

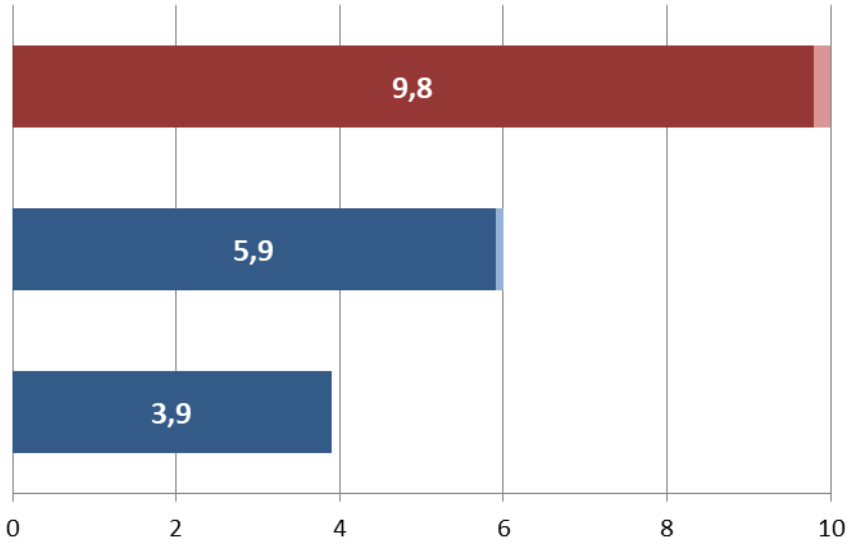
Debian

https://security-tracker.debian.org/tracker/CVE-2020-7247

Mitre CVE ID

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7247

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 sono stati raggiunti i seguenti punteggi:

- *Base Score:* 9,8
- *Impact:* 5,9
- *Exploitability:* 3,9

Vettore CVSS 3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/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.