Raport eveniment cibernetic

Vulnerabilitate Critică a OpenSSH

Vulnerabilitatea de securitate cibernetică a **OpenSSH (Secure Shell),** clasificată ca **CVE-2024-6387**, reprezintă o regresie a unei vulnerabilități mai vechi (**CVE-2006-5051**) pentru care producătorul a emis un patch de securitate în anul 2006.

Procesul serverului OpenSSH, **sshd** este vulnerabil la o condiție a handler-ului de semnale, permițând execuția de cod de la distanță neautentificat cu privilegii root pe sistemele Linux bazate pe glibc în configurația sa implicită.

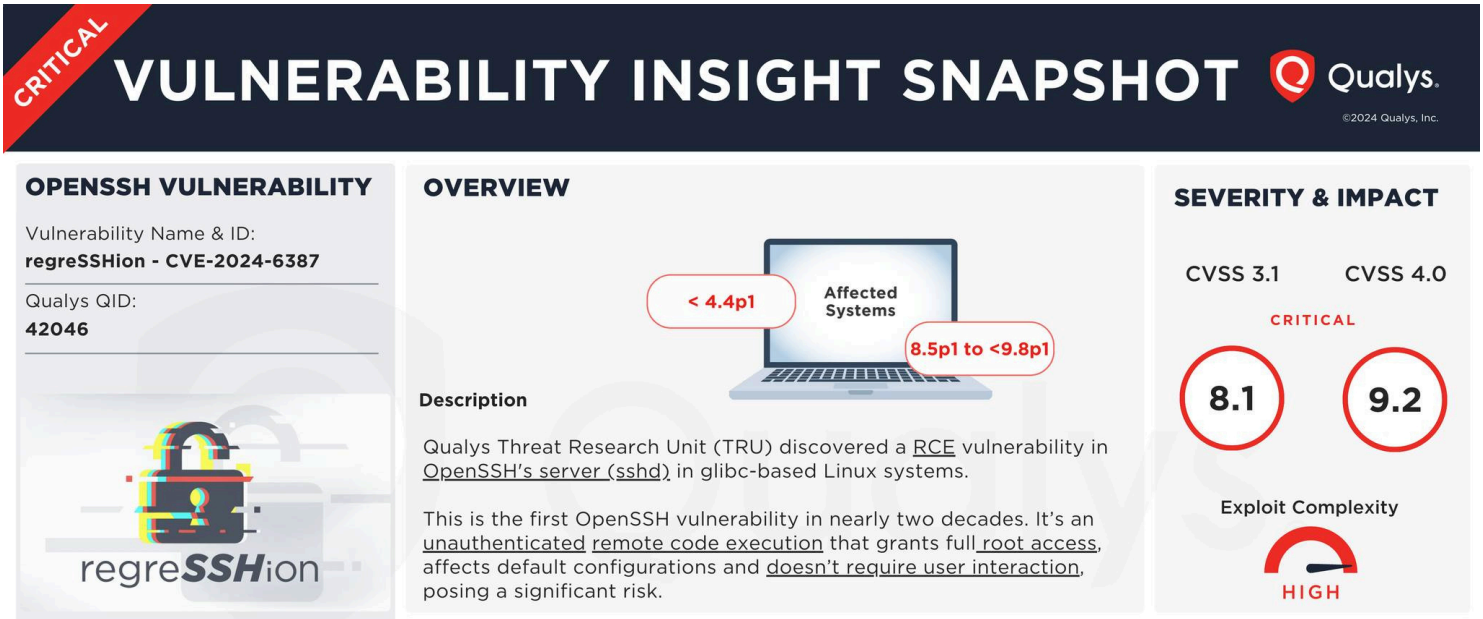

photo source : www.qualys.com

Această vulnerabilitate poate fi exploatată de la distanță pe sistemele Linux bazate pe glibc din cauza faptului că syslog() apelează funcții nesigure pentru semnale asincrone, precum malloc() și free(), conducând la execuția de cod neautentificat de la distanță ca root.

Aceasta se întâmplă deoarece codul privilegiat al sshd nu este izolat și rulează cu privilegii complete. OpenBSD nu este vulnerabil deoarece handler-ul său pentru semnalul de alarmă (SIGALRM) folosește syslog_r(), o versiune sigură pentru semnalele asincrone a syslog().

Informații sumare

TIP	**Vulnerabilitate cibernetică CVE**
Detalii tehnice	
Impact	Vulnerabilitatea CVE-2024-6387 afectează următoarele versiuni ale OpenSSH: ● **Anterioare 4.4p1**, dacă nu au fost corectate pentru vulnerabilitățile de securitate cibernetică CVE-2006-5051 și CVE-2008-4109; ● **De la 8.5p1 până la 9.8p1 (fără a include versiunea 9.8p1)**, din cauza eliminării accidentale a unei componente necesare în remedierea vulnerabilității. ● **Versiunile aplicației OpenSSH de la 4.4p1 până la 8.5p1 (fără a include versiunea 8.5p1)** nu sunt vulnerabile la CVE-2024-6387, datorită unei corecții efectuate la nivelul vulnerabilității CVE-2006-5051. Deși este mai dificil de exploatat, prin prisma faptului că necesită multiple încercări pentru lansarea unui atac cibernetic reușit, vulnerabilitatea CVE-2024-6387 poate genera prejudicii destul de importante asupra sistemelor informatice care rulează versiunile aplicației OpenSSH menționate.

***XQL query* identificare resurse afectate**	`// Query to identify hosts vulnerable to CVE-2024-6387`
	`preset = host_inventory_applications`
	`| filter endpoint_type = ENUM.AGENT_TYPE_SERVER`
	`| filter lowercase(application_name) ~= "openssh(-server)?"`
	`| alter product_major_version = to_number(arrayindex(split(raw_version, "."), 0)),`
	`product_minor_version_stage_1 = arrayindex(split(raw_version, "."), 1),`
	`product_rev = to_number(arrayindex(split(raw_version, "p"), 1))`
	`| alter product_minor_version = to_number(arrayindex(split(product_minor_version_stage_1, "p"), 0))`
	
	`// (name:"openssh" and version<4.4) or (name:"openssh" and version>=8.5)`
	`| filter product_major_version < 4 or (product_major_version = 4 and product_minor_version < 4) or (product_major_version = 8 and product_minor_version >= 5) or (product_major_version = 9 and product_minor_version < 8)`
	`| fields endpoint_name, application_name, raw_version, product_major_version, product_minor_version, product_rev`
	`| dedup endpoint_name`

Recomandări	
	Cel mai indicat mod de remediere a vulnerabilității OpenSSH îl constituie aplicarea de patch-uri de securitate pentru versiunile afectate. În vederea diminuării riscurilor de securitate, recomandăm întreprinderea următoarele măsuri: ● Gestionarea patch-urilor de securitate: aplicați rapid patch-urile disponibile pentru OpenSSH și prioritizați procesele de actualizare continuă; ● Controlul accesului: limitați accesul SSH prin controale bazate pe rețea pentru a minimiza riscurile de atac cibernetic.

Resurse externe

	• *https://unit42.paloaltonetworks.com/threat-brief-cve-2024-6387-openssh/* • *https://dnsc.ro/citeste/alerta-vulnerabilitate-critica-de-securitate-cibernetica-identificata-la-nivelul-aplicatiei-openssh*