TLP:CLEAR
Szabadon terjeszthető!

Tájékoztató
Linux szervereket érintő sérülékenységekről
(2024. november 25.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) tájékoztatót ad ki Linux drisztribúciókat ─ köztük Ubuntu webszervereket ─ érintő **magas kockázati besorolású** sérülékenységekről, az érintett szoftvertermékek széles körű elterjedtsége, valamint a sebezhetőségek súlyossága és kihasználhatósága miatt.

A Qualys LPE (local priviledge escalation) sebezhetőséget fedezett fel az egyes Linux disztribúciókban ─ szerver verziókat is beleértve ─ natívan megtalálható **needrestart** csomagban (CVE-2024-48990, CVE-2024-48991, CVE-2024-48992 és CVE-2024-11003), amelyek sikeres kihasználásuk esetén **root** szintű jogosultsági szint emelést tehetnek lehetővé. Továbbá ismerté vált a **libpsmodule-scandemodule-perl** sebezhetősége is (CVE-2024-10224), amely kódfuttatásra használható ki.

Ubuntu és Debian kiadásokhoz már elérhető a csomag biztonsági frissítése, **ezek telepítése haladéktalanul javasolt.**

Érintett kiadások és csomagverziók:

	Kiadás:	**Csomag:**	**Sérülékeny verzió:**
Ubuntu	**Xenial (16.04 LTS)**	**needrestart**	**<= 2.6-1**
		libmodule-scandeps-perl	**<= 1.20-1**
	Bionic (18.04 LTS)	**needrestart**	**<= 3.1-1ubuntu0.1**
		libmodule-scandeps-perl	**<= 1.24-1**
	Focal (20.04 LTS)	**needrestart**	**<= 3.4-6ubuntu0.1**
		libmodule-scandeps-perl	**<= 1.27-1**
	Jammy (22.04 LTS)	**needrestart**	**<= 3.5-5ubuntu2.1**
		libmodule-scandeps-perl	**<= 1.31-1**
	Noble (24.04 LTS)	**needrestart**	**<= 3.6-7ubuntu4.1**
		libmodule-scandeps-perl	**<= 1.35-1**
	Oracular (24.10)	**needrestart**	**<= 3.6-8ubuntu4**
		libmodule-scandeps-perl	**< 1.35-1**

Debian	**bullseye**	**needrestart**	**<3.5-4+deb11u4**
			< 1.30-1+deb11u1
	bookworm (security)	**needrestart**	**< 3.6-4+deb12u2**
		libmodule-scandeps-perl	**< 1.31-2+deb12u1**
	sid, trixie	**needrestart**	**< 3.7-3.1**
		libmodule-scandeps-perl	**< 1.35-2**

Az **apt list --installed | grep „^\(needrestart\|libmodule-scandeps-perl\)”** parancs futtatásával ellenőrizhető a rendszer érintettsége.

Mitigáció

Elsődlegesen javasolt megoldás a biztonsági javítást tartalmazó, frissített csomagok telepítése. Amennyiben ez nem megvalósítható, vagy az adott kiadáshoz nem érhető el még javítás, az alábbi mitigáció átmenetileg alkalmazható, azzal a figyelmeztetéssel, hogy a frissítés telepítése után javasolt visszaállítani az eredeti konfigurációt:

 # Disable interpreter scanners.

$nrconf{interpscan} = 0;

Hivatkozások:

- https://ubuntu.com/blog/needrestart-local-privilege-escalation
- https://www.openwall.com/lists/oss-security/2022/05/17/9
- https://www.qualys.com/2024/11/19/needrestart/needrestart.txt
- https://github.com/rschupp/Module-ScanDeps/security/advisories/GHSA-g597-359q-v529
- https://phrack.org/issues/55/7.html#article

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Incidensbejelentés: csirt@nki.gov.hu