禪

تهدیدات بحرانی برطرف شدند

دو آسیبپذیری با درجه بحرانی در Node.JS شناسایی شدند

Securing
node JS
TM

کارشناسان امنیتی موفق به شناسایی دو آسیبپذیری بحرانی امنیتی در Node.js شدند. آسیبپذیری اول منجر به پیادهسازی یک حمله منع دسترسی به سرویس میشود؛ بهطوری که به یک هکر اجازه میدهد یک حمله انکار سرویس را پیادهسازی کند . نسخههای 0.12 تا 5 این زبان به این آسیبپذیری آلوده هستند . این آسیبپذیری در رده 7.5 از 10 طبقهبندی شده است که نشان میدهد این آسیبپذیری تا چه اندازه بحرانی بوده است. مقیاس بحرانی بودن این آسیبپذیری در جدول زیر نشان داده شده است .

آسیبپذیری دوم در ارتباط با دسترسی غیرمجاز است؛ هر چند آسیبپذیری دوم نسبت به مورد اول بحرانی به شمار نمیرود؛ اما نسخههای x.4 و x.5 را شامل میشود. جدول زیر میزان مخاطرات این آسیبپذیری را نشان میدهد. با استفاده از این آسیبپذیری، یک هکر ممکن است توانایی دسترسی خارج از محدوده یا پیادهسازی یک حمله منع سرویس را روی یک برنامه جاوا اسکریپت داشته باشد .

Metric	Score
Base Score:	7.5 (High)
Base Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Attack Vector:	Network (AV:N)
Attack Complexity:	Low (AC:L)
Privileges Required:	None (PR:N)
User Interaction:	None (UI:N)
Scope of Impact:	Unchanged (S:U)
Confidentiality Impact:	None (C:N)
Integrity Impact:	None (I:N)
Availability Impact:	High (A:H)

Metric	Score
Base Score:	4.4 (Medium)
Base Vector:	CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H
Attack Vector:	Network (AV:N)
Attack Complexity:	Medium (AC:H)
Privileges Required:	High (PR:H)
User Interaction:	None (UI:N)
Scope of Impact:	Unchanged (S:U)
Confidentiality Impact:	Score
Integrity Impact:	4.4 (Medium)
Availability Impact:	CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H

هر چند این رخنه از درجه اهمیت کمتری برخوردار است؛ اما به هر ترتیب نصب وصلههای ارائه شده ضروری است؛ بر همین اساس بنیاد Node.js وصلههایی را برای ترمیم آسیبپذیریهای پلتفرم سمت سروری جاوا اسکریپت ارائه کرده است . در زمان نگارش این مقاله وصلههای مربوطه در اختیار کاربران قرار گرفته است و جای هیچگونه نگرانی وجود ندارد . سبک بودن و توانایی ایجاد محیطهای نرمافزارهای رویدادمحور و بلادرنگ باعث شده است، Node.JS نزد توسعهدهندگان وب، بسیار محبوب باشد مورد اول بحرانی به شمار نمیرود؛ اما نسخههای x.4 و x.5 را شامل میشود. جدول زیر میزان مخاطرات این آسیبپذیری را نشان میدهد.

نویسنده :
حمیدرضا_تائبی
دسته بندی:
امنیت
تاریخ انتشار :
18:06 - 05/11/1394
برچسب:
Node.JS - آسیبپذیری - DDoS

□□□□□ منبع: https://www.shabakeh-mag.com/security/2794