باسمه تعالی

آسیب پذیری عدم احراز هویت در Elasticsearch

فهرست مطالب

۱ مقدمه

Elasticsearch یک موتور تجزیه و تحلیل و جست‌وجو تمام متن و متن باز با مقیاس‌پذیری بالا است. این موتور جست‌وجو اجازه ذخیره، جست‌وجو و آنالیز سریع و تقریباً آنی حجم زیادی از اطلاعات را می‌دهد. این موتور جست‌وجو به طور کلی به عنوان موتور جستجو و پایگاه داده برنامه‌های قدرتمند و سرویس‌های آنلاین متعدد استفاده می‌شود.

۲ آسیب‌پذیری عدم احراز هویت در Elasticsearch

Elasticsearch به تنهایی از احرازهویت یا محدود ساختن دسترسی به انبار داده پشتیبانی نمی‌کند و پیاده-سازی یک حفاظ امنیتی مناسب را به توسعه‌دهندگان برای محیط‌هایشان واگذار کرده است. همچنین نسخه-های قبل از Elasticsearch 1.2 در پیکربندی پیش‌فرض خود اسکریپت‌نویسی پویا را فعال دارند که به مهاجمان از راه دور اجازه اجرای یک عبارات دلخواه MVEL و کد جاوا به عنوان قسمتی از کوئری از طریق ارسال پارامتر به search_ را می‌دهند.

این آسیب‌پذیری CVE-2014-3120 نام گذاری شده است. نمره CVSS پایه 6.8 به آن اختصاص داده شده است. رشته برداری CVSS آن (AV:N/AC:M/Au:N/C:P/I:P/A:P) است.

۳ محصولات تحت تأثیر آسیب‌پذیری

نسخه‌ی Elasticsearch 1.1.1 تحت‌تأثیر این آسیب‌پذیری قرار دارد. نسخه Elasticsearch 1.2 تحت‌تأثیر آسیب‌پذیری اجرای کد از راه دور قرار ندارد اما همچنان دارای نگرانی‌هایی امنیتی است.

۴ اقدامات جهت مقابله با آسیب‌پذیری

- خط زیر را جهت غیرفعال کردن اسکریپت‌نویسی پویا برای جلوگیری از اجرای کد از راه دور به فایل elasticsearch.yml اضافه کنید:

```
script.disable_dynamic: true
```

- همچنین باید مطمئن شوید که نمونه Elasticsearch محلی تان تنها بر روی localhost قابل اتصال است در غیر این صورت مهاجم می‌تواند از طریق LAN به پایگاه داده شما دست‌پیدا کند.
- با یک لایه پروکسی دسترسی به جست‌وجو و شاخص گذاری را محدود کنید.
- Elasticsearch را به آخرین نسخه ارتقاء دهید.
- Elasticsearch را پشت دیوارآتش قرار دهید.