# **API10:2019 پایش و نظارت ناکافی**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | |  | |  | |
| **خاص API** | **قابلیت بهره‌برداری: 2** | **میزان شیوع: 3** | **قابلیت تشخیص: 1** | **پیامد فنی: 2** | **خاص کسب‌و‌کار** |
| مهاجمین می توانند از فقدان فرایند ثبت وقایع و پایش برای سوءاستفاده پنهانی از سیستم‌ها بهره ببرند. | | بدون ثبت وقایع و پایش آنها یا با ثبت و پایش ناکافی، رهگیری فعالیت‌های مخرب و پاسخ آنها در زمان مناسب تقریبا غیرممکن خواهد بود. | | بدون پایش فعالیت‌های مخربی که در حال انجام است، مهاجمین زمان زیادی برای نفوذ به سیستم‌ها خواهند داشت. | |

**آیا API از نظر پایش و نظارت ناکافی[[1]](#footnote-1) ‌آسیب‌پذیر است؟**

در صورتی که یکی ازشرایط زیر وجود داشته باشد، API ‌آسیب‌پذیر خواهد بود:

* API هیچگونه Logای تولید نکند، سطح ثبت وقایع[[2]](#footnote-2) به درستی تنظیم نشده باشد یا پیام‌‌های Log، حاوی جزئیات کافی نباشند.
* جامعیت[[3]](#footnote-3) Logها تضمین نشده باشد (مثلا [Log Injection](https://www.owasp.org/index.php/Log_Injection) رخ دهد).
* Logها به طور پیوسته پایش نشوند.
* زیرساخت API به طور پیوسته پایش نشود.

**مثال‌‌هایی از سناریوهای حمله**

**سناریو #1**

کلیدهای دسترسی به یک API مدیریتی در یک انباره[[4]](#footnote-4) عمومی افشا شده و در اختیار همگان قرار گرفته است. مالک انباره از طریق یک ایمیل از این افشای احتمالی مطلع می‌شود اما بیش از 48 ساعت طول می‌کشد تا اقدام مقتضی انجام شود که در این حدفاصل، افشای کلید دسترسی ممکن سبب دسترسی غیرمجاز به داده حساس شده باشد. از آنجا که پایش کافی وجود نداشته است، سازمان نخواهد توانست بفهمد عوامل مخرب به چه داده‌ای دسترسی پیدا کرده‌اند.

**سناریو #2**

یک پلتفرم اشتراک گذاری ویدئو با یک حمله درج هویت[[5]](#footnote-5) در مقیاسی بزرگ مواجه می‌شود. علیرغم آنکه تلاش‌‌های ناموفق ورود ثبت می‌شوند، اما هیچگونه هشداری در طول زمان حمله اعلام نشده است؛ بلکه تنها در واکنش به شکایت‌‌های کاربران، Logهای API تحلیل و حمله کشف شده است. در نتیجه سازمان مجبور به صدور اعلامیه‌ای رسمی شده و از تمامی کاربران می‌خواهد که گذرواژه‌‌های خود را تغییر دهند. همچنین سازمان بایستی به مراجع نظارتی درخصوص این حادثه گزارش داده و پاسخگوی آنها باشد.

**API10:2019 پایش و نظارت ناکافی**

**چگونه از ‌آسیب‌پذیری پایش و نظارت ناکافی پیشگیری کنیم؟**

* تمامی تلاش‌‌های ناموفق احراز هویت، دسترسی‌‌های غیرمجاز و خطاهای اعتبارستجی ورودی[[6]](#footnote-6) بایستی ثبت[[7]](#footnote-7) شوند.
* Logها باید به گونه ای تهیه شوند که توسط راهکارهای مدیریت Log قابل استفاده بوده و همچنین جزئیات کافی جهت شناسایی عامل مخرب را در خود داشته باشند.
* با Logها بایستی به عنوان داده حساس رفتار شده و جامعیت آنها هم در زمان ذخیره سازی و هم در زمان انتقال تضمین شود.
* یک سیستم پایش پیکربندی و راه اندازی شود تا بتوان بطور مداوم و پیوسته عملکرد زیرساخت، شبکه و API را پایش نمود.
* از یک سیستم مدیریت رویدادها و اطلاعات امنیتی (SIEM) برای تجمیع و مدیریت Logهای دریافتی از تمامی مولفه‌‌های پشته API و میزبان‌‌های آن استفاده شود.
* از Dashboardها و هشدارها یا اعلان‌‌های سفارشی‌سازی شده به منظور تشخیص و پاسخ سریع به فعالیت‌‌های مشکوک استفاده شود.

**مراجع**

**OWASP**

* [OWASP Logging Cheat Sheet](https://www.owasp.org/index.php/Logging_Cheat_Sheet)
* [OWASP Proactive Controls: Implement Logging](https://owasp.org/www-project-proactive-controls/)
* [OWASP Application Security Verification Standard: V7: Error Handling and Logging Verification Requirements](https://github.com/OWASP/ASVS/blob/master/4.0/en/0x15-V7-Error-Logging.md)

**خارجی**

* [CWE-1059: Incomplete Documentation](https://cwe.mitre.org/data/definitions/1059.html)
* [OpenAPI Initiative](https://www.openapis.org/)

1. Insufficient Monitoring [↑](#footnote-ref-1)
2. Logging Level [↑](#footnote-ref-2)
3. Integrity [↑](#footnote-ref-3)
4. Repository [↑](#footnote-ref-4)
5. Credential Stuffing [↑](#footnote-ref-5)
6. Input Validation [↑](#footnote-ref-6)
7. Log [↑](#footnote-ref-7)