

گزارش حادثه برای SOC

نویسنده : سینا محبی

چگونه یک گزارش حادثه برای مرکز عملیات امنیت بنویسیم



**نمونه گزارش حادثه برای SOC**

**برای دانلود نسخه Docx به لینک زیر مراجعه کنید:**

**https://blog.sinamohebi.com**

[**https://www.linkedin.com/in/sinamohebi**](https://www.linkedin.com/in/sinamohebi/)

**تمامی اطلاعات درج شده در این سند غیرواقعی بوده و صرفا جهت ارائه نمونه گزارش حادثه برای مرکز عملیات امنیت تهیه شده است.**



Date  
1402/06/10

Incident report

### حق تألیف

این سند صرفا جهت ارائه به واحد SOC تهیه و تدوین شده است و کلیه حقوق مادی و معنوی آن متعلق به شرکت نورانت میباشد . نشر و کپی برداری از آن بدون اجازه کتبی از این شرکت ممنوع میباشد.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **کد شناسه** | **طبقه­بندی** | **تعداد صفحات** | **تاریخ تنظیم** | **ویرایش** |
| SOC Incident-report 1402-06-10 | محرمانه | 6 | 1402-06-10 | 1.0 |

|  |  |
| --- | --- |
| **تهیه کننده گزارش** | **زمان شیفت** |
| سینا محبی  Mohebi@nooranet.com | عصر |

**اطلاعات اولیه حادثه**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| شرح حادثه | تاريخ و ساعت | مبدا حمله | مقصد حمله | تأثير حادثه | سيستم هدف |
| تشخيص حمله SQL Injection | ۱۴۰۲-۰۶-۱۰  از ساعت ۱۶:۵۵ الی ۱۷:۰۹ | 40.80.148.42 | 192.168.250.70 | دسترسی و کسب اطلاع مقادیر از پایگاه داده بدون احراز هویت | وب سرور Microsoft IIS 8.5 |

**شرح حادثه**

با توجه به بررسی‌های صورت گرفته توسط تیم مرکز عملیات امنیت و با بهره‌گیری از داشبوردهای امنیتی موجود در SIEM متوجه گردید در ساعت۱۶:۵۵ الی ۱۷:۰۹ دقیقه از مبدا**40.80.148.42** به مقصد **192.168.250.70** حمله SQL Injection صورت گرفته است با توجه به ادامه بررسی‌ها مشخص گردید مهاجم با استفاده از ضعف امنیتی و دور زدن مکانیزم‌های دفاعی مانند WAF توانسته است کدهای مخرب خود را سمت وب سرور سازمان اجرا کند. همچنین مشخص گردید مبدا این حملات جزو آدرس های مخرب روی اینترنت بوده.

**شرح فنی حادثه**

در بررسی‌های صورت گرفته روی داشبورد تشخیص شناسایی حملات وب مشخص گردید از مبدا **40.80.148.42** تعداد زیادی درخواست مخرب حمله SQL injection از نوع Retrieval hidden information و Time base SQL injection روی سرور های سازمان صورت گرفته است که می‌توانید در تصویر زیر بخشی از این پیلودهای مخرب را مشاهده کنید.

A screenshot of a computer

Description automatically generated

تصویر 1 نمونه از درخواست های مخرب XSS

همانطور که در تصویر بالا مشاهده می کنید مهاجم با ارسال مقادیر مخرب که در ادامه به آن ها اشاره می شود در تلاش بوده است که این حمله را اجرا کند.

مقادیر مخرب در فیلد Uri\_query :

;select%20pg\_sleep(10)

(select(0)from(select(sleep(6))

از این مقادیر برای حملات ذکر شده استفاده می شود. همچنین جهت اطمینان از صحت این اطلاعات از منابعی مانند :

<https://github.com/payloadbox/sql-injection-payload-list>

<https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SQL%20Injection>

استفاده شده است تا از صحت تشخیص این داشبورد اطمینان حاصل نمود.

همچنین مشخص گردید که از این مبدا تعداد ۱۷۸ درخواست مخرب دریافت شده است که متاسفانه هیچ کدام از مکانیزم های دفاعی مانند  WAF قادر به شناسایی آنها نبوده است و این درخواست های مستقیما به وب سرور سازمان رسیده است.

**تاثیر حادثه**

با توجه به این که این حمله موفقیت آمیز بوده است، تاثیر آن به شرح زیر است :

* عبور از مکانیزم های دفاعی مانند WAF
* برقراری ارتباط با پایگاه داده بدون احراز هویت و کسب دسترسی
* کسب اطلاع از مقادیر و داده های حساس و طبقه بندی شده در پایگاه داده
* دسترسی به اطلاعات هویتی کاربران

**پاسخگویی به حادثه**

با توجه به حساسیت داده ها و مخرب تشخیص دادن این فعالیت ها، آدرس مبدا این درخواست ها توسط فایروال به مدت ۲۴ ساعت مسدود گردید.

همچنین با بررسی مبدا این درخواست ها توسط وب سایت abuseipdb.com مشخص گردید که این مبدا این درخواست ها در لیست آدرس های مخرب اینترنتی قرار داشته است که می توانید در تصویر زیر مشاهده کنید.

A screenshot of a computer

Description automatically generated