SONY

Prepared By: Gopi Gor

Date: 10/13/2023

THREAT INTEL REPORT

Hype Value	General Risk	Risk to SONY
High	Low Risk	Medium Risk

Title: SONY Data Breach in the U.S.

Date: October 13, 2023

Threat description:

Sony recently encountered a data breach that impacted multiple people in the United States. The compromise happened on May 28, but it was finally discovered only in June, early on. This breach unveiled personal information about employees and their families, which was close to about 7000 individuals. The exploitation took place due to a zero-day vulnerability in the MOVEit Transfer platform. The platform is a transfer platform to send and receive files between businesses.

A zero-day vulnerability is a vulnerability, one that is not ideally known by the developers of the system. It can be exploited till it is discovered and fixed. This was the zero-day that was discovered and fixed for the data breach that happened in Sony. This vulnerability allows unauthorized access to the MOVEit platform.

CVE-2023-34362	SQL injection (Remote Code Execution

The below table shows the affected versions of the MOVEit Transfer platform which was exploited through the SQL injection.

Affected Version	**Fixed Version**
MOVEit Transfer 2023.0.0	MOVEit Transfer 2023.0.1
MOVEit Transfer 2022.1.x	MOVEit Transfer 2022.1.5
MOVEit Transfer 2022.0.x	MOVEit Transfer 2022.0.4
MOVEit Transfer 2021.1.x	MOVEit Transfer 2021.1.4

SONY

Impact:

An attacker can use the SQL injection technique and get unauthorized access to a database through the MOVEit transfer platform. They can also manipulate the database as required.

Risk Assessment:

Based on the information, the risk to SONY is Medium Risk. This vulnerability was discovered on the MOVEit platform, so if SONY were to use the platform only then would it pose a risk to the company.

We know that SONY uses the platform for their file transfer, and it is used by most employees, thus posing a medium risk to the company. This vulnerability uses remote code execution to launch the SQL injection. The current vulnerability was patched, but there is a possibility which could be another zero-day vulnerability posing a risk to SONY.

Actions taken:

1. Took the platform offline and fixed the vulnerability.
2. Got a team of cybersecurity experts to launch an investigation.
3. Notified law enforcement.
4. Increased monitoring of all systems.
5. The breached recipients were notified individually, offered credit monitoring and identity restoration services with unique code.

Next steps and recommended actions:

1. Monitor account statements.
2. Review credit history for unauthorized transactions.
3. Constant upgrades to software's and platforms.

Sources:

1. https://www.bleepingcomputer.com/news/security/sony-confirms-data-breach-impacting-thousands-in-the-us/
2. https://www.bleepingcomputer.com/news/security/new-moveit-transfer-zero-day-mass-exploited-in-data-theft-attacks/