|  |
| --- |
| Zorg Industries |
|  |

# Memorandum

To: Andrew Ryan

From: Hari Seldon

CC: Chad Ballay; Hunter Goncalves; Jordan Smelser; Diane Yablonski

Subject: Fortnight 2019 Vulnerability - Lessons Learned

We have reviewed the available information around the recent Fortnite breach and have prepared the following report for you.

**Overview**

On January 16, 2019, Check Point researchers identified that an older/unused domain(<http://ut2004stats.epicgames.com>) allowed for arbitrary JavaScript to run. (XSS vulnerability) This JavaScript would be triggered by the intended victim clicking a malicious URL created by the attacker. In doing so this URL and the XSS vulnerability would activate the next stage of this breach. Epic Games wrote their own and for this situation incorrect implementation of Single Sign-On(SSO). The combination of these items allowed for the sending of an unsanitized URLredirect to be processed and then would send the SSO credentials for the user to the attacker. With those SSO credentials, the attacker would have complete access to the account. Stealing of in game currency, holding the account for ransom, using the account for a staging point for attacks against the victim’s social graph.

A screenshot of a cell phone

Description automatically generated

Figure Attack Flow Diagram

**Original Source Analysis of Fortnite Vulnerability**

<https://research.checkpoint.com/hacking-fortnite/>

**Highlevel breakdown of Fortnite Vulnerability**

* Unused but online sub domains provided internal staging point.
* XSS exploit used to inject malicious JavaScript.
* WAF failed to block these requests.
* SSO implementation reflected users’ credentials due to unsanitized input.

OWASP Top Ten alignment (1, 2, 5, and 7)

<https://owasp.org/www-project-top-ten/>

**Response**

User education with a focus on ensuring a consistent message to not click links from unknown person(s) should be reviewed. (<https://nvd.nist.gov/800-53/Rev4/control/AT-2>)

A prioritization of inventorying all of our domains and subdomains should be taken immediately. (<https://nvd.nist.gov/800-53/Rev4/control/CM-8>)

A prioritization of reviewing the completeness of our vulnerability scans should be taken after the domain and subdomain census. (<https://nvd.nist.gov/800-53/Rev4/control/CA-7>)

A technical review of our own SSO implementation should be done immediately followed by an additional third party review when allowed. (<https://nvd.nist.gov/800-53/Rev4/control/IA-2>)

Tabletop exercise using our own Incident Response Plan with this scenario as a basis is advised. (<https://nvd.nist.gov/800-53/Rev4/control/CP-4>)

**Summary**

An action plan will be forthcoming to work through the iterated list above. Once this internal review is complete, we will send a follow-up. If during the review process any actionable items occur, we will include yourself on the communications so that you can remain aware of resolution.