AppSec/SR/2021-08/38

Advisory – Broken/External Links can be Disastrous
Release date: August 26, 2021
Severity & Impact: High
Source: Centre of Excellence for Application Security, Jaipur

Systems Affected:
All Websites/Applications hosted in NIC Data Centers

Overview & Description

In a recent finding, a third party site link given on a Government website was found to be redirected to a site having malicious/forbidden contents.

On detailed investigation, it was revealed that earlier, the redirected domain was owned by the Government Department itself, which was discontinued and surrendered subsequently.

Later on this domain was registered by an unidentified entity, who deployed malicious/forbidden contents on it.

Since the link was not removed from the Government Website, it started redirecting to a domain having malicious/forbidden contents.

Recommendations:

1. All Websites/Applications should immediately be checked for any broken links and be removed, if any.
2. The redirection to any other site/third party Website/Application should be with an appropriate disclaimer.
3. All External/third party URL links in the WebSite/Application should be regularly checked for authenticity of the contents.

References:

- https://monsido.com/blog/how-fix-broken-links-your-website
- https://www.wordstream.com/blog/ws/2010/06/02/how-to-find-and-fix-broken-links