Advanced Notification of Cyber Threats against Microsoft SharePoint Servers

Security Advisory	ADV-19-19	**Criticality**	High	
Advisory Released On	13 May 2019			

Impact

An exploit that allows unauthenticated attackers to run arbitrary code in the SharePoint application pool and the SharePoint server farm account.

Solution

Adhere the advices written under the recommendations section.

Affected Platforms:

- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Foundation 2013 SP1
- Microsoft SharePoint Server 2010 SP2
- Microsoft SharePoint Server 2019

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found out about a critical vulnerability in Microsoft SharePoint software. The exploit targets a vulnerability (CVE-2019-0604) that was recently patched by Microsoft. The re-exploit of Microsoft SharePoint software may be leveraged through a remote code execution vulnerability that occurs when the software fails to check the source markup of an application package thus, leading to the execution of arbitrary code on the SharePoint application pool and the SharePoint server farm account.

Details

Microsoft SharePoint has many architectures in its context, and due to the exploited security flaw with checking the source markup of an application package, attackers have managed to craft special code which resulted with several changes on the context of the SharePoint application pool and the SharePoint server farm account.

The first step the attacker takes in order to exploit the vulnerability is through the use of the crafted encoded package.

One of the vulnerabilities is exploited through the XmlSerializer. Typically considered a secure serializer, it is possible to be exploited if the attacker can manipulate the expected type; this is done by analyzing the XmlSerializer(Type) constructor calls. One of the methods – or functions – that call the constructor is the following:

```
Microsoft.SharePoint.BusinessData.Infrastructure.EntityInstanceIdEncoder.DecodeEntityInstanceId(string)
```

This method is found in `Microsoft.SharePoint.dll`.

The next step is to trace through the calls and look for one that originates from a point that can be initiated externally, as well as check if the argument value can be provided.

After that is completed, the attacker tries to pick an entity alongside the ability to edit the entity and load a post data on by using several strings.

Lastly, the attacker can use this method to select the object to edit through the use of `PickerEntity`, and then edit the object and post his or her own modified data through the use of `EntityEditor.LoadPostData(string, NameValueCollection)`.

Recommendations

In order to circumvent the exploit, we highly recommend the following:

- Frequently download the latest patches released by Microsoft.
- If no patches are available, vulnerable SharePoint servers should be placed behind a firewall in order to prevent external access.

Disclaimer

Accessing third-party links in this advisory will direct you to an external website. Please note that aeCERT bears no responsibility for third-party website traffic. aeCERT will have no liability to the entities for the content or use of the content available through the hyperlinks that are referenced

References

Zero Day Initiative - CVE-2019-0604

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 777 4003
Fax (+971) 4 777 4100
Email info[at]aeCERT.ae
Instagram @TheUAETRA
Twitter @TheUAETRA

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae