Advanced Notification of Cyber Threats against Elastic Services Controller Vulnerability

aeCERT
فريق الاستجابة لطوارئ الحاسب الآلي
Computer Emergency Response Team

Security Advisory	ADV-19-16	**Criticality**	High	○○○●
Advisory Released On	9 May 2019			

Impact

Exploiting the vulnerability allows unauthenticated remote attacker to take full control over the affected system.

Solution

Adhere the advices written under the recommendations section.

Affected Platforms:

- ESC version 4.1 up-to ESC version 4.4

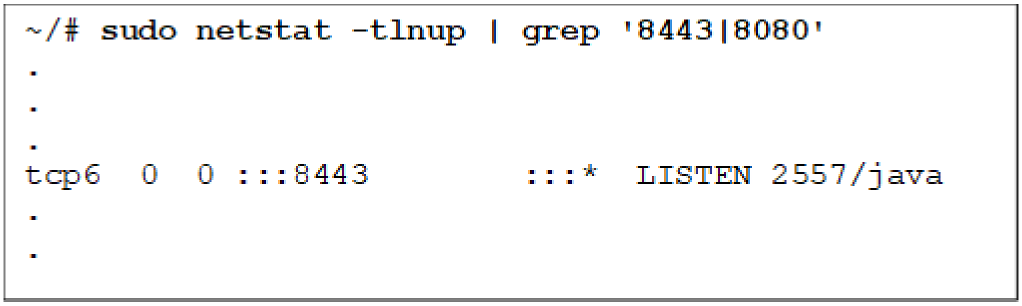
Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found about a critical vulnerability within Cisco virtual network functions manager tool, the Elastic Services Controller (ESC). The exploit of ESC vulnerability may be leveraged through REST API. Calls to REST API on a vulnerable machine can be used to bypass authentication and take full control of the affected system. This vulnerability is present when REST is enabled on the system. All ESC virtual machines with Software Release from 4.1 to 4.4 are vulnerable. Cisco has addressed this vulnerability by releasing an updated software of ESC 4.5.

Details

Cisco ESC provides proper controls to manage all aspects of Virtual Network Functions. The cause of vulnerability is due to improper authentication of API requests on the software releases 4.1, 4.2, 4.3, and 4.4. The attacker can exploit the vulnerability by sending crafted a HTTP request to the REST API – the REST API allows for communication between a web-based client and a server. If the breach was successful, the attacker can perform and execute arbitrary actions through the REST API with administrative privileges on vulnerable systems.

The exploitation of this vulnerability can only occur where REST API is enabled. REST API is not enabled by default. To identify whether REST API is enabled, the output of the command below indicates the REST API is enabled on port 8443.



```
~/# sudo netstat -tlnup | grep '8443|8080'
.
.
.
tcp6   0   0 :::8443          :::*   LISTEN 2557/java
.
.
```

Recommendations

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

Cisco has released software update that addressed the mentioned vulnerability. We recommend updating your software as soon as possible.

The vulnerability is fixed in version 4.5 and above.

In cases where applying the software update is not possible, to avoid the exploit ensure to disable REST API on the affected device.

References

Cisco

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