Advanced Notification of Cyber Threats against Exploits Targeting SAP Applications

Security Advisory	ADV-19-13	**Criticality**	High	
Advisory Released On	02 May 2019			

Impact

A vulnerability in SAP applications that could be exploited by attackers eliminating the need to have user credentials to access the system.

Recommendations

Adhere the advices written under the recommendations section.

Affected Platforms

- SAP Applications

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has gotten insight of a major vulnerability in SAP applications that can be exploited by hackers in order to gain access to systems without the need to have user credentials.

Threat Details

aeCERT has become aware of several exploits targeting SAP applications due to a vulnerability that has recently been publicly released. The exploits would allow attackers to gain access to the system resulting in espionage, sabotage, and financial fraud attacks. Based on research, 90% of SAP customers who are currently running ABAP-based systems are deemed vulnerable. It is foreseen that the majority of the SAP attacks would be targeted towards business-critical applications in use through the deployment of these exploits.

In order to exploit the system, an attacker would only need the IP address of the SAP system that is being targeted in aims to either steal data or shut the system down. User credentials are not required thus, the act itself is carried out remotely. The vulnerability could be exploited on both unsecured and default installations as well as SAP systems including S/4HANA that have been hardened by bypassing ACLs.

If you require further details, you can refer to the presentation found in the references section.

Solution

For exploit **remediation**, follow the security measures below:

- Restrict authorized hosts via ACL file on MS internal pointed by profile parameter ms/acl_info.
- Split MS internal/public: rdisp/msserv=0 & rdisp/msserv_internal=39NN.
- Avoid exposing MS internal port (tcp/39NN) to clients.
- Enable SNC for clients.

For exploit **detection**, keep an eye on the security measures below:

- ms/audit=1|2 + dev_ms file monitoring.
- Network flow monitoring on 32NN, 33NN, 39NN.
- http(s)://<msg_serv_host>: <msg_serv_http_port>/msgserver/text/logon.
- Transaction SMMS

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

FireEye

OPCDE presentation

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