CYBERSECURITY ADVISORY

# New Exploits for Unsecure SAP Systems

**Last Revised:** May 03, 2019 **Alert Code:** AA19-122A



## Summary

The Cybersecurity and Infrastructure Security Agency (CISA) is issuing this activity alert in response to recently disclosed exploits that target unsecure configurations of SAP components. [1 <https://github.com/msuiche/opcde/tree/master/2019/emirates/(sap)%20gateway%20to%20heaven%20-%20dmitry%20chastuhin%2c%20mathieu%20geli>]

# Technical Details

A presentation at the April 2019 Operation for Community Development and Empowerment (OPCDE) cybersecurity conference describes SAP systems with unsecure configurations exposed to the internet. Typically, SAP systems are not intended to be exposed to the internet as it is an untrusted network. Malicious cyber actors can attack and compromise these unsecure systems with publicly available exploit tools, termed “10KBLAZE.” The presentation details the new exploit tools and reports on systems exposed to the internet.

## SAP Gateway ACL

The SAP Gateway allows non-SAP applications to communicate with SAP applications. If SAP Gateway access control lists (ACLs) are not configured properly (e.g., gw/acl_mode = 0), anonymous users can run operating system (OS) commands.[2] According to the OPCDE presentation, about 900 U.S. internet-facing systems were detected in this vulnerable condition.

## SAP Router secinfo

The SAP router is a program that helps connect SAP systems with external networks. The default `secinfo` configuration for a SAP Gateway allows any internal host to run OS commands anonymously. If an attacker can access a misconfigured SAP router, the router can act as an internal host and proxy the attacker’s requests, which may result in remote code execution.



According to the OPCDE presentation, 1,181 SAP routers were exposed to the internet. It is unclear if the exposed systems were confirmed to be vulnerable or were simply running the SAP router service.

### SAP Message Server

SAP Message Servers act as brokers between Application Servers (AS). By default, Message Servers listen on a port 39XX and have no authentication. If an attacker can access a Message Server, they can redirect and/or execute legitimate man-in-the-middle (MITM) requests, thereby gaining credentials. Those credentials can be used to execute code or operations on AS servers (assuming the attacker can reach them). According to the OPCDE presentation, there are 693 Message Servers exposed to the internet in the United States. The Message Server ACL must be protected by the customer in all releases.

### Signature

CISA worked with security researchers from Onapsis Inc.[3 <https://www.onapsis.com/>] to develop the following Snort signature that can be used to detect the exploits:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"10KBLAZE SAP
Exploit execute attempt"; flow:established,to_server;
content:"|06 cb 03|"; offset:4; depth:3;
content:"SAPXPG_START_XPG"; nocase; distance:0; fast_pattern;
content:"37D581E3889AF16DA00A000C290099D0001"; nocase;
distance:0; content:"extprog"; nocase; distance:0; sid:1;
rev:1;)
```

Give Feedback

# Mitigations

CISA recommends administrators of SAP systems implement the following to mitigate the vulnerabilities included in the OPCDE presentation:

- Ensure a secure configuration of their SAP landscape.

- Restrict access to SAP Message Server.
  - Review SAP Notes 1408081 and 821875. Restrict authorized hosts via ACL files on Gateways (`gw/acl_mode` and `secinfo`) and Message Servers (`ms/acl_info`).[4], [5]
  - Review SAP Note 1421005. Split MS internal/public: `rdisp/msserv=0` `rdisp/msserv_internal=39NN`. [6]
  - Restrict access to Message Server internal port (`tcp/39NN`) to clients or the internet.
  - Enable Secure Network Communications (SNC) for clients.
- Scan for exposed SAP components.
  - Ensure that SAP components are not exposed to the internet.
  - Remove or secure any exposed SAP components.

# References


[1] Comae Technologies: Operation for Community Development and Empowerment (OPCDE) Cybersecurity Conference Materials <https://github.com/msuiche/opcde/tree/master/2019/emirates/(sap)%20gateway%20to%20heaven%20-%20dmitry%20chastuhin%2c%20mathieu%20geli>

[2] SAP: Gateway Access Control Lists

[3] Onapsis Inc. website <https://www.onapsis.com>

[4] SAP Note 1408081

[5] SAP Note 821875

[6] SAP Note 1421005


# Revisions

**May 2, 2019:** Initial version

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

## Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

**Topics** </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

**News & Events** </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

**CISA Central**

1-844-Say-CISA contact@cisa.dhs.gov

Give Feedback

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

Give Feedback