

VANGUARD

Integrity Professionals, Inc.

Enterprise Security Software

z/OS IBM CICS Transaction Server for ACF2 STIG

Version: 6

Release: 4

29 Dec 2020

Group ID (Vulid): V-17982

Group Title: ZB000021

Rule ID: SV-43225r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZCICR021

Rule Title: IBM CICS Transaction Server SPI command resources will be properly defined and protected.

Vulnerability Discussion: IBM CICS Transaction Server can run with sensitive system privileges, and potentially can circumvent system controls. Failure to properly control access to product resources could result in the compromise of the operating system environment, and compromise the confidentiality of customer data. Many utilities assign resource controls that can be granted to system programmers only in greater than read authority. Resources are also granted to certain non systems personnel with read only authority.

Responsibility: Information Assurance Officer

IAControls: ECCD-1

Check Content:

Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITVE.RPT(XCMD)
- ACF2CMDS.RPT(RESOURCE) Alternate report

Automated Analysis:

Refer to the following report produced by the ACF2 Data Collection Checklist:

- PDI (ZCIC0021)

Ensure that all IBM CICS Transaction Server SPI command resources are properly protected according to the requirements specified in CICS SPI Resources table in the z/OS STIG Addendum. If the following guidance is true, this is not a finding.

The ACF2 resources and/or generic equivalent as designated in the above table are defined with a default access of PREVENT.

The ACF2 resource access authorizations restrict access to the appropriate personnel as designated in the above table.

Fix Text: nsure that the IBM CICS Transaction Server SPI command resource access is in accordance with those outlined in CICS SPI Resources table in the zOS STIG Addendum.

Use CICS SPI Resources and CICS SPI Resources Descriptions tables in the zOS STIG Addendum. These tables list the resources and access requirements for IBM CICS Transaction Server; ensure the following guidelines are followed:

The ACF2 resources and/or generic equivalent as designated in the above table are defined with a default access of PREVENT.

The ACF2 resource access authorizations restrict access to the appropriate personnel as designated in the above table.

The following commands are provided as a sample for implementing resource controls:

```
$KEY(ASSOCIATION) TYPE(XCD)
- UID(CICSAUDT) SERVICE(READ) ALLOW
- UID(CICUAUDT) SERVICE(READ) ALLOW
- UID(SYSCAUDT) SERVICE(READ) ALLOW
- UID(*) PREVENT
```

CCI: CCI-000035

CCI: CCI-002234

UNCLASSIFIED