2019 januari examen

1. Order 4 problemen op de niveau van ernstigheid.

A. Cross-site scripting (XSS) vulnerability in the management interface for VMware ESX 2.5.x before 2.5.2 upgrade patch 2, 2.1.x before 2.1.2 upgrade patch 6, and 2.0.x
before 2.0.1 upgrade patch 6 allows remote attackers to inject arbitrary web script or HTML via messages that are not sanitized when viewing syslog log files.
CVE-2005-3619

B. The default configuration of VMware Workstation 6.0.2, VMware Player 2.0.x before 2.0.3, and VMware ACE 2.0.x before 2.0.1 makes the console of the guest OS accessible
through anonymous VIX API calls, which has unknown impact and attack vectors.
CVE-2008-1392

C. VMware Workstation 8.x before 8.0.2, VMware Player 4.x before 4.0.2, VMware Fusion 4.x before 4.1.2, VMware ESXi 3.5 through 5.0, and VMware ESX 3.5 through 4.1 use an
incorrect ACL for the VMware Tools folder, which allows guest OS users to gain guest OS privileges via unspecified vectors.
CVE-2012-1518

D. Airwatch Agent for Android contains a vulnerability that may allow a device to bypass root detection. Successful exploitation of this issue may result in an enrolled
device having unrestricted access over local Airwatch security controls and data.
CVE-2017-4895

=> A < C < D < B

2. Attack Tree: Geef zo veel mogelijk manieren waarop je de klantenlijst van een bedrijf op de cloud kunt stelen.

3. Geef min. 6 voorbeelden uit teksten of eigen voorbeelden of van uit de les van multilevel/defense in depth

4. Bespreking project

5. Vraag over welk hoofdstuk dat je gelezen hebt.

Revision #1
Created 31 October 2021 22:23:35 by Jasper G.

Updated 16 January 2022 15:02:33 by Jasper G.