Is my EFT Arcus implementation susceptible to the Azure Stack vulnerabilities?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT Arcus

QUESTION

Is my EFT Arcus implementation susceptible to the Azure Stack vulnerabilities?

ANSWER

No. EFT Arcus does not use Azure Stack Hub integrated system.

A security company called CheckPoint purposefully attempts to exploit popular software to identify vulnerabilities, and then notify the software developers to patch it before customers' systems are attacked. They successfully infiltrated the Azure Stack, then informed Microsoft of the vulnerability, and Microsoft promptly patched the software before any customers were affected.

MORE INFORMATION

The exploits are described at the links below:

CVE-2019-1372

A remote code execution vulnerability exists when Azure Stack fails to check the length of a buffer prior to copying memory to it. An attacker who successfully exploited this vulnerability could allow an unprivileged function run by the user to execute code in the context of NT AUTHORITY\system thereby escaping the Sandbox. The security update addresses the vulnerability by ensuring that Azure Stack sanitizes user inputs.

CVE-2019-1234

A spoofing vulnerability exists when Azure Stack fails to validate certain requests. An attacker who successfully exploited the vulnerability could make requests to internal Azure Stack resources. An attacker could exploit the vulnerability by sending a specially crafted request to the Azure Stack user portal. The update addresses the vulnerability by changing

how Azure Stack handles certain requests.