Multiple Vulnerabilities in Cisco UCS Director and Cisco UCS Director Express for Big Data

Executive Summary

Cisco identified multiple critical vulnerabilities in the REST API of Cisco Unified Computing System (UCS) Director and Cisco Unified Computing System (UCS) Director Express for Big Data. These vulnerabilities may allow a remote attacker to bypass authentication or conduct directory traversal attacks on an affected device. The Cisco UCS Architecture is integral to the Epic Electronic Health Record solution for many HPH entities.[i, ii, & iii] Patches and updates are available from Cisco, and HC3 recommends applying them to resolve these vulnerabilities.

Analysis

Cisco UCS Director and UCS Director Express for Big Data Authentication Bypass Vulnerability

A vulnerability in the REST API of Cisco UCS Director and UCS Director Express for Big Data (CVE-2020-3243, CVE-2020-3250, both CVSS 9.8 – Critical) could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions with administrative privileges on an affected device.[iv & v]

The vulnerability is due to insufficient access control validation. An attacker could exploit this vulnerability by sending a crafted request to the REST API. A successful exploit would allow the attacker to interact with the REST API with administrative privileges, potentially causing Denial of Service (DoS) condition on the affected device.

Cisco UCS Director and UCS Director Express for Big Data Remote Code Execution Vulnerability

A vulnerability in the REST API of Cisco UCS Director and UCS Director Express for Big Data (CVE-2020-3243, CVSS 9.8 – Critical), could allow an authenticated, remote attacker to execute arbitrary code with *root* privileges on the underlying operating system. Root privileges provide system-level (i.e. 'super-user') access to all resources on a system.

The vulnerability is due to improper input validation. An attacker could exploit this vulnerability by crafting a malicious file and sending it to the REST API. A successful exploit would allow the attacker to open a remote shell and execute code with *root* privileges.

Cisco UCS Director and UCS Director Express for Big Data Directory Traversal Vulnerability

A vulnerability in the REST API of Cisco UCS Director and UCS Director Express for Big Data (CVE-2020-3239, CVE-2020-3247, CVE-2020-3248, CVE-2020-3249, and CVE-2020-3251, each CVSS 9.8 – Critical) could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device. [vi, vii, viii, & ix]

The vulnerability is due to insufficient validation of user-supplied input to the REST API of the affected software. An attacker could exploit this vulnerability by sending a crafted request to the REST API. A successful exploit would allow the attacker to execute code on the system, allow the attacker to perform a Denial of Service (DoS) attack on the affected device, allow the attacker to execute code with *root* privileges, or allow the attacker to write or execute arbitrary files on the system with full administrative privileges.

Cisco UCS Director Directory Traversal Vulnerability

A vulnerability in the REST API endpoint of Cisco UCS Director (CVE-2020-3252, CVSS 9.8 – Critical) could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device.[x]

The vulnerability is due to insufficient validation of user-supplied input to the REST API of the affected software. An attacker could exploit this vulnerability by sending a crafted request to the REST API. A successful exploit would allow the attacker to read arbitrary files on the system.

Patches & Mitigations

Patches and Updated Releases

Cisco has released free software updates and updates that address each of the vulnerabilities, UCS Director Release 6.7.4.0 and UCS Director Express for Big Data Release 3.7.4.0.[xi] HPH entities are encouraged to patch and update all systems affected by these vulnerabilities.

References

[i] Delaney, M. (2018). Complementary Upgrades Help Hospitals Get the Most out of EHR Deployments. Accessed 16 April 2020 at https://healthtechmagazine.net/article/2018/08/complementary-upgrades-help-hospitals-get-most-out-ehr-deployments

[ii] Mellor, C. (2018). If you're NetApp-y and you know it, clap your hands. If you're app-y and you know it… FlexPods get application layers, managed service – and more. The Register. Accessed 16 April 2020 at https://www.theregister.co.uk/2018/06/07/netapp_flexpod_applications/

[iii] Cisco. (2016). Solution Brief: Epic on Cisco UCS®: Helping Healthcare Providers Do More, Faster, and at a Lower Cost. Intel.com. Accessed 16 April 2020 at https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/epic-on-cisco-helping-healthcare-providers-solution-brief.pdf

[iv] National Vulnerability Database. (2020). CVE-2020-3243. NVD.NIST.gov. Accessed 16 April 2020 at https://nvd.nist.gov/vuln/detail/CVE-2020-3243

[v] National Vulnerability Database. (2020). CVE-2020-3250. NVD.NIST.gov. Accessed 16 April 2020 at https://nvd.nist.gov/vuln/detail/CVE-2020-3250

[vi] National Vulnerability Database. (2020). CVE-2020-3251. NVD.NIST.gov. Accessed 16 April 2020 at https://nvd.nist.gov/vuln/detail/CVE-2020-3251

[vii] National Vulnerability Database. (2020). CVE-2020-3239. NVD.NIST.gov. Accessed 16 April 2020 at https://nvd.nist.gov/vuln/detail/CVE-2020-3239

[viii] National Vulnerability Database. (2020). CVE-2020-3247. NVD.NIST.gov. Accessed 16 April 2020 at https://nvd.nist.gov/vuln/detail/CVE-2020-3247

[ix] National Vulnerability Database. (2020). CVE-2020-3248. NVD.NIST.gov. Accessed 16 April 2020 at https://nvd.nist.gov/vuln/detail/CVE-2020-3248

[x] National Vulnerability Database. (2020). CVE-2020-3252. NVD.NIST.gov. Accessed 16 April 2020 at https://nvd.nist.gov/vuln/detail/CVE-2020-3252

[xi] Cisco. (April 15 2020). Multiple Vulnerabilities in Cisco UCS Director and Cisco UCS Director Express for Big Data. Cisco Security Advisories. Accessed 16 April 2020 at https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsd-mult-vulns-UNfpdW4E