Security Advisory 2022-030

Cisco Umbrella Virtual Appliance Vulnerability

April 22, 2022 — v1.0

TLP:WHITE

History:

- *22/04/2022 — v1.0 – Initial publication*

Summary

On the 20th of April Cisco released a security advisory about a high severity vulnerability in the key-based SSH authentication mechanism of Cisco Umbrella Virtual Appliance (VA). The vulnerability could allow an unauthenticated, remote attacker to impersonate a VA. Cisco has released software updates that address this vulnerability [1].

Technical Details

CVE-2022-20773 (CVSS Score: Base 7.5)

This vulnerability is due to the presence of a static SSH host key. An attacker could exploit this vulnerability by performing a man-in-the-middle attack on an SSH connection to the Umbrella VA. A successful exploit could allow the attacker to learn the administrator credentials, change configurations, or reload the VA. SSH is not enabled by default on the Umbrella VA [1].

There is no known public exploit of this vulnerability at the time that the advisory released.

Products Affected

This vulnerability affects the Cisco Umbrella Virtual Appliance for both VMWare ESXi and Hyper-V running a software version earlier than 3.3.2.

Recommendations

According to Cisco, depending on the version of the product it advised that

- Cisco Umbrella Virtual Appliance 3.2 and earlier should migrate to a fixed release.
- Cisco Umbrella Virtual Appliance 3.3 should update to 3.3.2

Workarounds

There are no workarounds that address this vulnerability.

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uva-static-key-6RQTRs4c