Verkada

March 9, 2021 Security Incident Report

Kyle Randolph, CISO
kyle.randolph@verkada.com

Martin Hunt, CTO
martin@verkada.com

1 Introduction

Upon learning of a security incident on March 9, 2021, Verkada immediately undertook response and mitigation activities, which included investigation of the incident. This report discusses Verkada's immediate response to the incident and what its investigation has shown regarding the extent of unauthorized access to customer data.

2 Executive Summary

From March 8-9, 2021, attackers compromised Verkada's platform and accessed customer data, including video, for a subset of Verkada customers. In all, 97 customers had their cameras accessed and video or image data viewed. Eight of those customers had Access Control product data accessed, including badge credentials. Separately, eight customers had their wifi credentials accessed. In total, this represents less than two percent of Verkada's approximately 6,000 customer population. Finally, the attackers downloaded a list of Command users (including names and email addresses but no passwords) and a list of Verkada sales orders.

The attackers' vector of entry was through a misconfigured customer support server exposed to the internet. Once the attackers accessed that server, they found customer support administrator credentials and used those to log into a customer support web interface, where they accessed customer devices using internal support functionality that emulated user sessions. Apart from this access, there was no other access to Verkada's internal network, including its financial systems and other business systems.

Verkada learned of the breach on March 9 at approximately 18:00 UTC. Within two hours, Verkada cut off the attackers' access, and within six hours Verkada began notifying affected customers.

Verkada engaged Perkins Coie LLP to provide legal advice regarding this incident. Thereafter, Perkins Coie retained FireEye/Mandiant to undertake a forensic investigation to assist Perkins.

3 Detection and Analysis

3.1.
Attribution

The attack has been attributed to a threat actor named Tillie Kottman. Past breaches allegedly associated with Kottmann have been consistent with opportunistic exploitation rather than a mission requiring sustained persistent access. On March 18, 2021, the U.S. Department of Justice announced that a federal grand jury had indicted Kottmann for conspiracy to commit computer fraud and abuse, conspiracy to commit wire fraud, and aggravated identity theft pertaining to activity that predated the attack on Verkada. The federal grand jury indictment alleges that Kottmann is a Swiss computer hacker who has hacked dozens of companies and government agencies and has purportedly leaked internal files and records of more than 100 entities.

3.2.
Determining Affected Customers

Our investigation set out to determine the upper bound of all possible unauthorized access to customer data and customer devices. As an upper bound (worst case), we include all data on any systems accessed by the attacker, even if there was limited or no evidence that any data was exfiltrated.

There were two systems directly involved in the attack. We describe both below with the scope of data that was exposed.

Customer Support (Jenkins) Server

The Verkada support team used a customer support server for remote customer support on behalf of customers. (For example, a customer might request assistance regarding underexposed video scenes, and the support team would use a script to adjust the exposure compensation of the cameras.) The customer support server did not contain production systems or any source code.

Network logs for this server show a total of 4GB of outbound data transfer. There was a total of 12GB of data on the customer support server containing customer support scripts and logs from script executions. Some of these logs contained customer data. It is unknown which, if any, customer data was exfiltrated from this server but, for the purposes of this report, we have taken a worst-case stance and assumed all data was exfiltrated. In total, 29 organizations had image files exposed through this server.

Command Support Web Interface

The customer support server contained admin-level credentials for executing support scripts. The attackers were able to use these credentials to access a support web interface. This web interface is typically used by (1) Verkada technical support employees to provide customer support, and (2) Verkada software engineers to debug customer issues. From this interface, the attackers downloaded:

- A list of client account users, including names and email addresses. This list did not include passwords or password hashes.

- A list of Verkada sales orders. Verkada's Command system normally uses sales order information to maintain the current state of licenses for customers. This information was obtained from the Command system and not from other Verkada business systems.

In total, the attackers accessed 68 customer organizations through the Command interface. Access Control product data, including badge credentials, for 8 organizations was potentially accessed. There were 4,530 cameras across these organizations which the attackers may have accessed. This figure represents a worst-case/upper-bound estimate based on any data being sent to the attacker's web browser including not only video, but also low-resolution preview thumbnails. No cameras were viewed for more than 90 minutes, and in the worst case estimate, cameras were viewed for an average of 11 minutes and a median time of four minutes. It is not known exactly how much live video was accessed due to limited information in log files. The attackers created six video archives on the Verkada platform and accessed 87 video archives. Fifteen People Analytics searches for images of persons were performed in five organizations. The search results in four of those organizations may have returned user-entered text labels associated with images of a person.

3.3. Devices

Device Firmware Integrity

All customer devices were reviewed for suspicious or unauthorized processes. The integrity of each device's root filesystem and firmware was verified by checking hashes against an expected set. The integrity check was run before and after a fleet-wide reboot of devices.

Device Metadata

Some device metadata, e.g., device serial number or model name, was exposed for the aforementioned 97 organizations through both the Command web interface and the Jenkins server.

Cameras

There is no evidence of tampering with or deletion of video/image data stored on cameras.

The attackers sent remote non-interactive shell commands to 25 cameras in six customer organizations. The commands were basic reconnaissance like whoami and ping. No evidence of backdoors or lateral movement was discovered in our logs.

Other Devices

No evidence of remote access or tampering was found for devices in the Access Controller (AC), Sensor (SV), or Viewing Station (VX) product lines.

3.4. AWS

The Jenkins Server, Support Web Interface, and other Verkada Command infrastructure are hosted in AWS. There is no evidence that the attackers accessed AWS or any AWS credentials except for a call to AWS KMS to decrypt the support-script password and a few calls to list resources like S3 buckets.

There is no evidence of any access or lateral movement to other AWS servers.

3.5. Customer User Passwords for the Command Platform

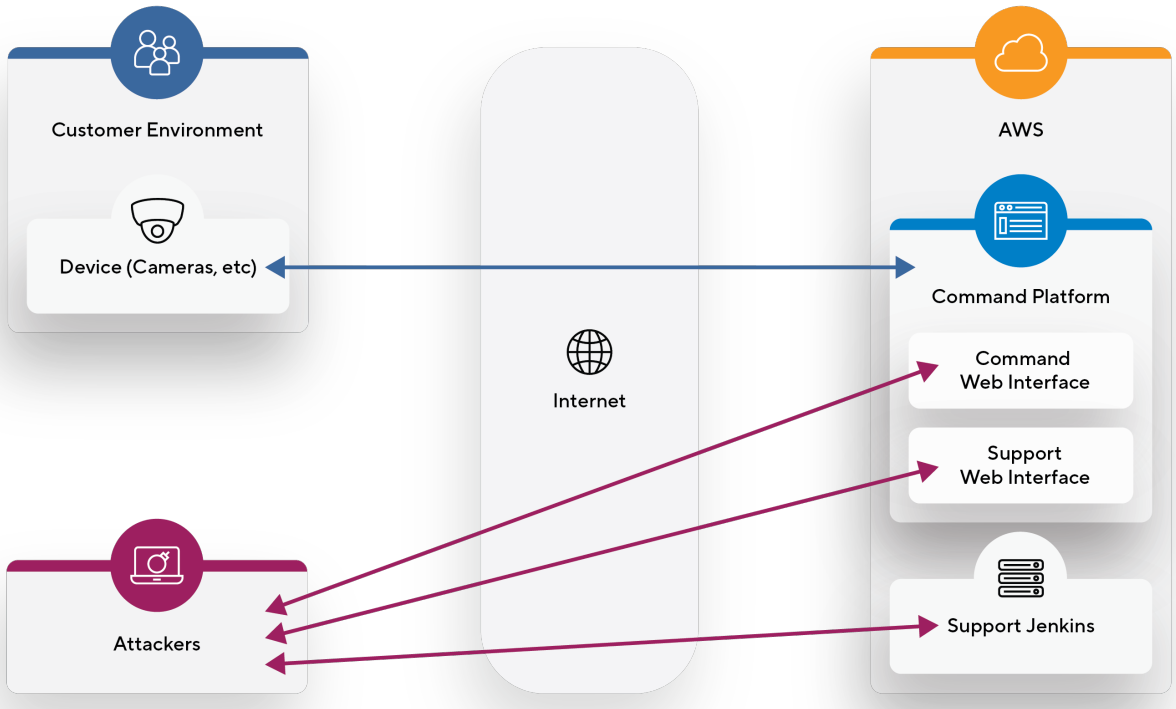
There was no evidence of access to the datastore where user password hashes for the Command platform are stored.

4 Response Communications

On March 9, Verkada notified all customers of the incident via email. Soon thereafter, all potentially affected customers were sent the findings of our investigation including the specific customer data of theirs that may have been exposed. Updates on the incident investigation were emailed to customers and posted to https://www.verkada.com/security-update.

Appendix

Brief Architecture Overview



Verkada's customer support team used an internet-facing Jenkins server to perform common customer support actions such as batch updating a setting on a set of cameras.

Verkada's primary application platform, the Command Platform, is where users manage their devices and organizations and view data from their devices such as live and historical camera video.

The Command Platform had a Support Web Interface that the technical support team and engineering team used for troubleshooting customer issues and fixing bugs.

Devices hosted in the customer's environment, such as cameras, access control devices, sensors and viewing stations, communicate with the Command Platform to receive commands, configuration settings, and firmware updates, as well as send video data and logs.

Vendors

Perkins Coie LLP is a leading international law firm that provides a full array of corporate, commercial litigation, data breach response, and regulatory legal services to a broad range of clients.

FireEye is a cybersecurity company known for its security technology products, threat intelligence, and Mandiant Consulting professional services.