Municipal Surveillance Infrastructure as a Cybersecurity Target: Lessons from Traffic Camera Vulnerabilities in Tehran, Iran

Tiffany Rad
ELCnetworks, LLC
March 6, 2026

Abstract

Urban traffic camera systems are a foundational component of modern intelligent transportation infrastructure. However, the network connectivity that enables these capabilities also introduces cybersecurity risks. Recent reporting indicates that foreign intelligence services exploited Tehran's municipal traffic camera network to track individuals prior to targeted strikes.[i] In March of 2026, the *Financial Times* reported that hacked traffic cameras were utilized to target Ali Khamenei; exploitation on traffic cameras was done to track the movements of Khamenei, his security, and others close in his cabinet.[ii] A "pattern of life" was established as a result of foreign intelligence groups exploiting surveillance technologies, like traffic cameras. Paired with other data sets such as security guards' addresses, work hours, who was transportation and along which routes, this creates patterns than can be identified and predicted. In the case reviewed in this paper, Iran utilized these cameras to surveil their citizens; however, adversaries used these cameras to track and target Iranian government agents. After an anticipated regime change, successors will also have vulnerable cameras in their transportation infrastructure which could potentially be used for future surveillance.

Although the specific vendor of the exploited cameras has not been publicly identified, the incident highlights the intelligence value of municipal surveillance infrastructure and the potential risks posed by potentially exploitable vulnerabilities in these systems. Often, vulnerabilities result from failures to patch systems and from errors made during improper installation and configuration of these technologies.

This article analyzes publicly disclosed vulnerabilities in Bosch IP traffic cameras, focusing on CVE-2023-39509, a command injection vulnerability that allows authenticated administrators to execute arbitrary commands on camera operating systems. These traffic cameras are installed around the world, including in the United States. By examining the technical characteristics of this vulnerability and the broader threat landscape for networked surveillance devices, this paper explores how similar weaknesses could enable intelligence gathering or cyber operations against municipal infrastructure. The analysis concludes with recommendations for mitigating these risks through improved firmware management, network segmentation, and administrative security practices.

Introduction

Cities deploy traffic camera networks to manage congestion, monitor road conditions, enforce traffic laws, and support emergency response operations. However, these systems also function as powerful surveillance technologies capable of collecting continuous visual data about vehicles, locations, and individuals moving through urban environments. In Iran, traffic camera infrastructure has been integrated into broader state surveillance systems and used not only for transportation management but also for social monitoring. Authorities have reportedly used roadway cameras and related technologies to identify and track individuals, including women who do not comply with the Islamic Republic's mandatory dress code requirements and to identify government protestors. This dual use of traffic camera networks illustrates how transportation infrastructure can become part of a wider surveillance apparatus, raising important security and privacy concerns when such systems are vulnerable to cyber intrusion or misuse.

This integration has also expanded the attack surface of municipal infrastructures. Network-connected cameras often contain embedded operating systems, remote management interfaces, and connectivity to centralized command platforms. As a result, vulnerabilities within camera firmware or configuration environments may create opportunities for exploitation.

Recent articles indicate that foreign intelligence services may have accessed Tehran's municipal traffic camera network to track the movements of individuals prior to conducting targeted military strikes. The *Financial Times* reports that almost all of the traffic cameras in Tehran had been, "…hacked for years, their images encrypted and transmitted to servers in Tel Aviv and southern Israel." While specific traffic camera manufactures have not been publicly identified, the research highlights the potential intelligence value of municipal surveillance infrastructure. Compromised camera networks could enable adversaries to monitor vehicle movements, observe security patterns, and collect sensitive data about individuals or locations. If Iranian traffic cameras were exploited and accessed by foreign intelligence agencies, there is a concern that the same could be done elsewhere.

This research examines vulnerabilities in Bosch IP traffic camera firmware as a case study to illustrate how such systems may be exploited if not properly secured. The camera was chosen because after accessing open source web scraping tools, vulnerable cameras – some with remote access still enabled – were found after a search conducted on February 4, 2026. The goal is not to assert that Bosch cameras, specifically, were exploited by foreign intelligence services in Tehran, but rather to demonstrate how known vulnerabilities in widely deployed surveillance systems could theoretically enable similar exploitation scenarios. Other traffic and surveillance cameras in Iran, such as some manufactured in China, were also observed as part of this research.

The results highlight how the failure to apply available security patches and configuration errors during system installation remain common challenges across the cybersecurity landscape. These issues are not unique to Bosch products but reflect broader operational risks associated with managing networked devices. Ensuring that firmware is regularly updated and that systems are securely configured is a critical responsibility for municipal operators. Proper maintenance and configuration management can significantly reduce the likelihood that known vulnerabilities will be exploited in traffic camera and surveillance infrastructure.

Traffic Camera Networks as Intelligence Platforms

Urban traffic camera systems have expanded significantly in recent decades with the widespread adoption of intelligent transportation systems (ITS). These systems typically consist of networked cameras positioned throughout city roadways, centralized traffic management platforms, automated video analytics capabilities, remote configuration interfaces, and integration with law enforcement databases. Together, these components allow municipalities to monitor and manage traffic conditions in real time while collecting data that can support transportation operations.

Because these systems are distributed across urban environments and connected to centralized networks, they provide a persistent surveillance capability capable of generating large volumes of data about vehicle and pedestrian movement. This extensive coverage and connectivity can create opportunities for malicious actors if the systems are not properly secured or are installed with misconfigurations. Misconfigurations are common in in traffic infrastructures including traffic cameras and sometimes connected Advanced Traffic Controllers (ATC) which are the "brain" of a traffic intersection and is encased in boxes next to traffic intersections. Cybersecurity standards for the ATC, and other technologies in the transportation infrastructure , are critical because these comprise part of U.S. critical infrastructure.[iii]

If adversaries gain unauthorized access to traffic camera networks, they may be able to exploit these systems for intelligence-gathering purposes and also pivot into unprotected connected city networks. For intelligence services or sophisticated cyber actors, the combination of broad geographic coverage, continuous monitoring, and network connectivity makes traffic camera networks an attractive platform for surveillance and information collection.

Methodology

This research examines publicly available vulnerability disclosures and security advisories related to networked surveillance cameras. The analysis focuses specifically on Bosch IP camera firmware vulnerabilities published in 2010 2019, and 2023, with particular attention given to the vulnerability identified as CVE-2023-39509. This vulnerability was selected as a case study to better understand how weaknesses in network-connected surveillance devices could potentially be exploited within municipal infrastructure.

The analysis draws on several primary sources, including vendor security advisories issued by manufacturers, records from the Common Vulnerabilities and Exposures (CVE) database, publicly available reporting related to traffic camera infrastructure in Iran[iv], and technical documentation associated with Bosch products. By reviewing these materials, the research seeks to evaluate how the identified vulnerability might be exploited in real-world municipal deployments and to assess the potential cybersecurity implications for critical infrastructure systems that rely on networked surveillance technologies.

In 2023, an article was published stating that traffic cameras were being used in Tehran primarily for population surveillance technologies. European companies, such as Bosch, were at criticized for selling traffic cameras to Iran.[v] This research originated from that article by reviewing which cameras were installed in Iran and considering the inherent vulnerability in supply chains for products used in critical infrastructure.

Vulnerability Analysis: CVE-2023-39509

Bosch cameras were chosen in this analysis because of reporting stating that these were sold to Iran in 2023. Bosch Security Systems disclosed CVE-2023-39509 in Security Advisory BOSCH-SA-638184-BT. The vulnerability affects Bosch IP cameras running firmware from the CPP13 and CPP14 product families.

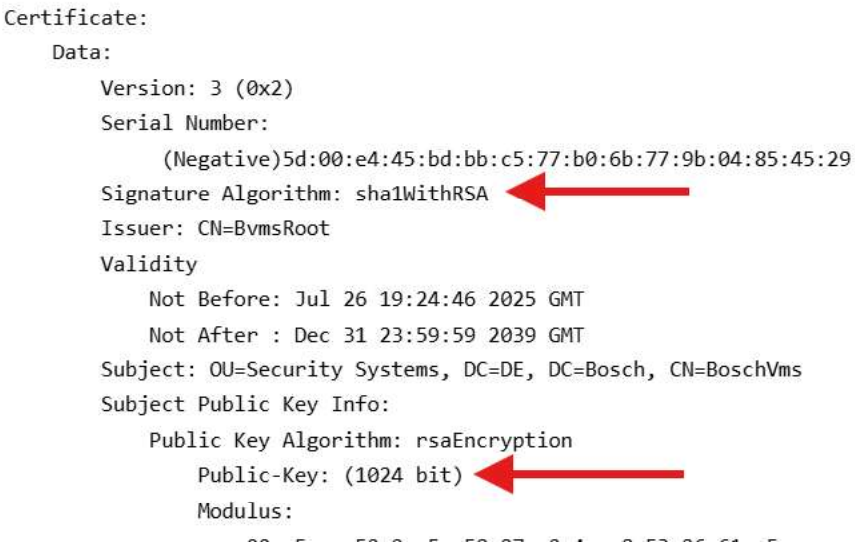
The vulnerability is classified as a command injection flaw resulting from improper input validation (CWE-20). An authenticated user with administrative privileges can exploit the vulnerability to execute arbitrary commands on the camera's operating system. The vulnerability has a CVSS v3.1 base score of 7.2, categorized as "high severity."

The affected firmware versions include CPP13 firmware versions ≤ 8.90 and CPP14 firmware versions 8.20–8.81. If exploited, the vulnerability could allow attackers to gain control of camera systems, manipulate configurations, extract data, or install malicious software.

Because many traffic camera deployments rely on centralized administrative control systems, compromise of administrator credentials could enable exploitation across large numbers of devices simultaneously.

Bosch cameras in the Shiraz traffic infrastructure were found operating on servers with vulnerabilities dating to 2010. The following information was accessed via Shodan on March 3, 2026:

SSL Certificate



Analysis

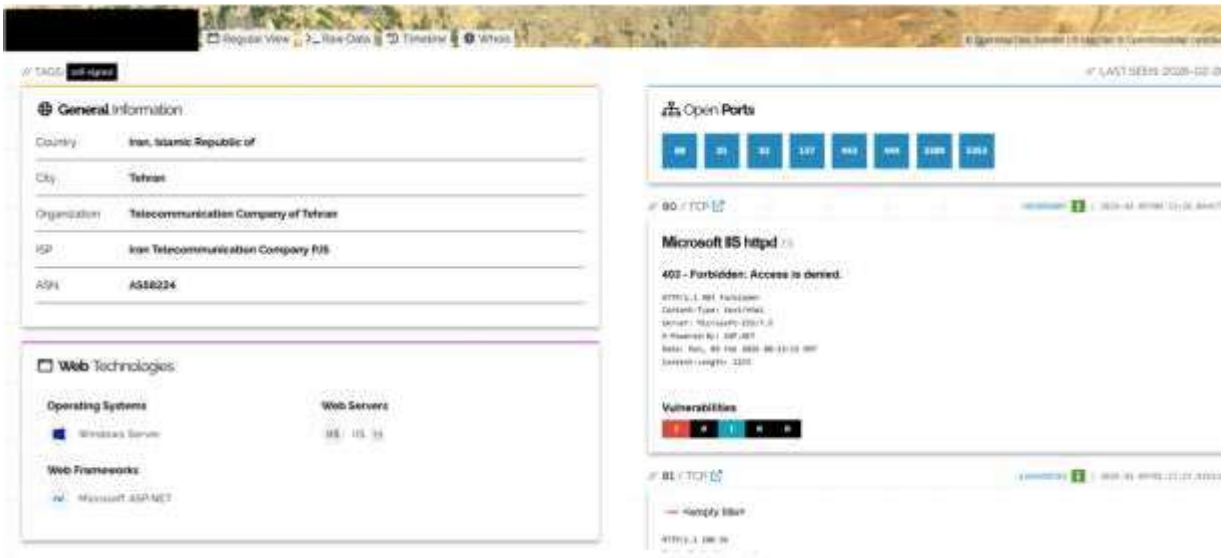
This is Bosch's VideoJet/VCS embedded web server used in surveillance cameras and video encoders. Exposing the server type can create a fingerprinting risk, because attackers can identify the device model or firmware family and search for known vulnerabilities. In secure deployments, organizations should remove or obfuscate server identification headers.

The keys show security weaknesses due to their weakness (1024-bit RSA, SHA-1, long validity) typical of older embedded surveillance hardware. 1024-bit RSA is considered insecure and was deprecated in 2014. It also uses a deprecated hash with signature algorithm: sha1WithRSAEncryption and has been deprecated due to collision vulnerabilities. The certificate has a long validity (2026-2034), which is not currently a recommended practice, but sometimes is used for embedded devices by default. 1 to 3 years for a life span is a more modern cybersecurity practice.

This device has 2 high-risk CVEs: CVE-2010—3972 and CVE-2010-2730. These vulnerabilities may allow for execution of arbitrary code or cause a denial of service, an HTTP request header can trigger a buffer overflow, allowing a remote attacker to execute arbitrary code on the server allowing attackers to compromise the web server and potentially gain control over the system.

Chinese Dahua hardware is associated with lower end Bosch cameras, due to a strategic partnership between the two companies, dating back to 2013, that lasted until approximately 2020.[vi]

The following information was accessed via Shodan on March 3, 2026:



HTTP/1.1 200 OK

Server: VCS-VideoJet-Webserver

Connection: keep-alive

Content-Type: text/html

Accept-Ranges: bytes

Content-Length: 1834

Expires: 0

Set-Cookie: HcsoB=38a0285352c07754; path=/;

Dahua-based Network recorder:

Web Version: 3.2.3.116876

This is significant because the server is Internet facing, has multiple services exposed, some with critical vulnerabilities. The last time this camera was indexed was February 13, 2026. It was not possible to check to see if it is currently visible at the time this paper was authored because the Internet in Iran is down.

This has the same CVEs as the camera in Shiraz, except this also has high-risk CVE-20019-0708 with the vulnerability of remote code in Remote Desktop Services; an unauthenticated attacker may connect to the target system using RDP and sends specially crafted request.

This device is running an older Bosch camera or video management firmware with outdated cryptographic defaults. The key concerns are weak 1024-bit RSA certificate, deprecated SHA-1 hashing, self-signed factory certificate, HTTP Basic authentication, and an identifiable device platform.

Additional Vulnerabilities in Surveillance Camera Systems

In addition to CVE-2023-39509, several other vulnerabilities have been disclosed that affect networked surveillance devices. These include information disclosure vulnerabilities in which certain camera firmware versions allow attackers to retrieve sensitive configuration data, such as network settings and device parameters. Other issues involve unauthenticated data exposure, where attackers may gain access to video analytics information or event metadata without authentication. Some older firmware versions also lack proper authentication controls, allowing remote attackers to modify camera settings or obtain sensitive information without being properly authorized.

Additionally, hardware-level security risks have been identified in certain configurations, where enabling advanced features such as enhanced stream security options may introduce risks to embedded security hardware components. Collectively, these vulnerabilities underscore the importance of secure device configuration and the timely installation of firmware updates to mitigate potential security threats.

Misconfigured traffic cameras via “human error” can also create cybersecurity risks because these devices are often connected to larger municipal networks, and some via the ATC adding vulnerabilities into that system if not running on segmented networks. Weak configurations such as default passwords, exposed management interfaces, or improperly restricted network access can allow unauthorized users to access the cameras. Once compromised, attackers may view video feeds or use the device as a pivot to move deeper into connected networks and other traffic devices.

The Bosch Video Management System (BVMS) and its related components have experienced several documented security vulnerabilities, some of which could potentially be exploited if systems are not properly patched or are exposed to untrusted networks.[vii] For example, CVE-2020-6770 affected the BVMS Mobile Video Service and allowed an unauthenticated remote attacker to execute arbitrary code through the deserialization of untrusted data, potentially enabling attackers to run commands on the system hosting the video management software. Another vulnerability, CVE-2019-11684, involved the RCP+ server of Bosch Video Recording Manager (VRM) and allowed unauthenticated access to certificate data stored within the Windows operating system, receiving a critical severity score.

Additional issues have been identified in installation and client components of Bosch video software, including DLL search path vulnerabilities that could allow arbitrary code execution if malicious files were placed in certain directories. Bosch IP cameras integrated into BVMS environments have also had vulnerabilities, such as CVE-2023-39509, which allowed command injection by administrative users, and CVE-2022-41677, which could expose device configuration data. Although most of these vulnerabilities were identified by security researchers, the National Institutes of Standards and Technology (NIST), and subsequently patched by Bosch, unpatched or internet-exposed deployments in the wild could potentially be exploited, highlighting the importance of regular updates, secure configuration, and restricted network access in surveillance infrastructure systems.[viii]

Security Implications for Municipal Infrastructure

The potential exploitation of traffic camera networks raises several significant security concerns. Compromised cameras could enable attackers to conduct intelligence collection by monitoring vehicle movements and identifying patterns associated with specific individuals or locations. Unauthorized access to these systems may also allow adversaries to map infrastructure, revealing network architecture, device configurations, and operational procedures.

In addition, attackers with administrative access could manipulate systems by disabling cameras, altering video feeds, or interfering with traffic monitoring operations. Because traffic cameras are often connected to broader municipal networks, compromised devices may also facilitate lateral pivoting within those networks, providing an entry point for wider cyber intrusions. These risks underscore the importance of treating surveillance devices as components of critical infrastructure rather than merely peripheral equipment.

Mitigation Strategies

Reducing the risk of exploitation requires both technical and administrative controls. Installing vendor security updates is one of the most effective ways to mitigate known vulnerabilities, and vendors such as Bosch have released patched firmware versions addressing CVE-2023-39509 and others. Many of the Bosch cameras observed in this research were unpatched. Strong credential management is also essential, with administrative access restricted to trusted personnel and protected through authentication processes. Surveillance devices should be placed on segmented networks, so they are isolated from other municipal systems and not directly exposed to the public internet as some observed in this research. Administrators should also follow secure configuration practices, such as avoiding interaction with untrusted content while logged into device management interfaces and using secure configuration tools when available. Finally, municipal IT departments should continuously monitor surveillance devices for unusual activity and maintain logs to support investigation and forensic analysis if a security incident occurs.

Conclusion

Municipal traffic camera networks provide valuable capabilities for transportation management and public safety, but they also introduce cybersecurity risks when vulnerabilities remain unpatched. The case of Tehran's surveillance infrastructure illustrates the potential intelligence value of compromised camera systems.

The ability to remotely identify and fingerprint surveillance devices further increases these risks. Attackers can use publicly accessible scanning tools to locate traffic cameras or video management servers exposed on the internet and identify them through distinctive characteristics such as default certificates, firmware signatures, or web banners. Once identified, these systems may be targeted for exploitation through known vulnerabilities. Because traffic camera systems are often integrated with municipal networks, compromised devices may also serve as entry points for lateral pivoting into other government systems.

This ability to fingerprint devices creates a security concern for municipal infrastructure because attackers can quickly locate and map exposed traffic cameras or video management servers across the internet. Once identified, those systems may be targeted for known vulnerabilities, credential attacks, or reconnaissance activities. As a result, security practices recommend replacing factory certificates (and not self-signing, as was found here), restricting management interfaces to internal networks, and ensuring surveillance devices are not directly exposed to the public internet.

Examples in this paper showed how Iran deployed traffic camera networks not only for transportation management, but also as part of a broader state surveillance apparatus. Authorities have used traffic cameras and other digital monitoring tools to identify and track individuals, including detecting women in vehicles who do not comply with the country's mandatory dress code requirements.[ix] At the same time, the same surveillance infrastructure created unintended security risks for the Iranian government itself; surveillance technologies can be repurposed against the very institutions that deploy them. This case illustrates a broader cybersecurity risk associated with municipal surveillance systems: infrastructure originally designed for monitoring the public can become an intelligence source for hostile actors if the systems are compromised. Moreover, if political transitions or regime change occur, the same vulnerable surveillance infrastructure may remain in place and could be repurposed by successors to continue monitoring citizens, raising concerns about the security and governance of networked surveillance technologies.

At the time of publication, research identified vulnerable internet-connected cameras in several U.S. cities, including Washington, D.C.; Arlington, Virginia; Boston, Massachusetts; New York City; and San Francisco. These findings highlight important cybersecurity risks in the United States' intelligent transportation infrastructure.

References

Bosch Security Systems. (2023). *Security advisory BOSCH-SA-638184-BT.*

Common Vulnerabilities and Exposures. (2023). *CVE-2023-39509.*

Advanced Transportation Controller (ATC) Cybersecurity Project under the United States Department of Transportation (USDOT) Contract # DTFH61-16-D-00055, Work Order # 19-0403.

Endnotes

[i] Shalev, T., & Diamond, J. (2026, March 3). *Hacked traffic cameras and US intelligence: How a plot to kill Iran's supreme leader came together*. CNN. https://www.cnn.com/2026/03/03/middleeast/us-israel-plot-kill-iran-khamenei-latam-intl

[ii] *Inside the plan to kill Ali Khamenei.* (2026, March 3). *Financial Times*. https://www.ft.com/content/bf998c69-ab46-4fa3-aae4-8f18f7387836

[iii] Institute of Transportation Engineers. (n.d.). *Cybersecurity for the advanced transportation controller (ATC) standards*. https://www.ite.org/technical-resources/topics/standards/cybersecurity-for-the-atc-standards/

[iv] Weinthal, B. (2023, August 8). *Iran bought spy tech from German, Chinese and other firms*. Iran International. https://www.iranintl.com/en/202308081259

[v] Weinthal, B. (2023, August 7). Germany's Bosch alleged to aid Iran in spy tech targeting protestors. *Iran International*. https://www.iranintl.com/en/202308074447

[vi] *Dahua and Bosch collaborate to provide integrated solution.* (2013, August 30). *Security World Market*. https://www.securityworldmarket.com/me/Newsarchive/dahua-and-bosch-collaborate-to-provide-integrated-solution

[vii] Robert Bosch GmbH. (2020, January). *Security advisory: Deserialization of untrusted data in BVMS Mobile Video Service (CVE-2020-6770).* Bosch Product Security Incident Response Team. https://media.boschsecurity.com/fs/media/pb/security_advisories/bosch-sa-885551-bt_cve-2020-6770_securityadvisory_bvms-mvs_deserialization_of_untrusteddata.pdf

[viii] National Institute of Standards and Technology. (n.d.). *CVE-2019-11684: Improper access control in Bosch Video Recording Manager (VRM).* National Vulnerability Database. https://nvd.nist.gov/vuln/detail/CVE-2019-11684

[ix] Sinaiee, M. (2025, May 1). *With hijab warnings via text, Iran expands digital surveillance on women*. Iran International. https://www.iranintl.com/en/202505018922