Information On How to Report Security Issues

Protecting our customers from threats to their security is always an important task for FOSCAM. As a key player in global Networking and Smart Home markets, we will do our utmost to provide our users with secure stable products and services, and to strictly protect the privacy and security of their data.
We welcome and encourage all reports related to product security or user privacy. We will follow established processes to address them and provide timely feedback.

Report Vulnerabilities to FOSCAM

We strongly encourage organizations and individuals to contact FOSCAM's security team to report any potential security issue
To report a security or privacy vulnerability, please send an email to **support@foscam.com** with the product model and software version, describe the detailed security issue to us. FOSCAM will endeavor to respond to the report within 6 working days.
FOSCAM will need to obtain detailed information about the reported vulnerability to more accurately and quickly begin the verification process.

Responsible Reporting Guidelines

1. All parties to a vulnerability disclosure should comply with the laws of their country or region.
2. Vulnerability reports should be based on the latest released firmware, and preferably written in English.
3. Report vulnerabilities through the dedicated communication channel. FOSCAM may receive reports from other channels but does not guarantee that the report will be acknowledged.
4. Adhere to data protection principles at all times and do not violate the privacy and data security of FOSCAM's users, employees, agents, services or systems during the vulnerability discovery process.
5. Maintain communication and cooperation during the disclosure process and avoid disclosing information about the vulnerability prior to the negotiated disclosure date.
6. FOSCAM is not currently operating a vulnerability bounty program.

How FOSCAM Deals with Vulnerabilities

FOSCAM encourages customers, vendors, independent researchers, security organizations, etc. to proactively report any potential vulnerabilities to the security team. At the same time, FOSCAM will proactively obtain information about vulnerabilities in FOSCAM products from the community, vulnerability repositories and various security websites. In order to be aware of vulnerabilities as soon as they are discovered.
FOSCAM will respond to vulnerability reports as soon as possible, usually within <how many> business days.
FOSCAM Security will work with the product team to perform a preliminary analysis and validation of the report to determine the validity, severity, and impact of the vulnerability. We may contact you if we need more information about the reported vulnerability.
Once the vulnerability has been identified, we will develop and implement a remediation plan to provide a solution for all affected customers.
Remediation typically takes up to 90 days and in some cases may take longer.
You can keep up to date with our progress and the completion of any remediation activities.

FOSCAM will issue a security advisory when one or more of the following conditions are met:
1. The severity of the vulnerability is rated CRITICAL by the FOSCAM security team and FOSCAM has completed the vulnerability response process and sufficient mitigation solutions are available to assist customers in eliminating all security risks.

2. If the vulnerability has been actively exploited and is likely to increase the security risk to FOSCAM customers, or if the vulnerability is likely to increase public concern about the security of FOSCAM products, FOSCAM will expedite the release of a security bulletin about the vulnerability, which may or may not include a full firmware patch or emergency fix.

Information on Minimum Security Update Periods

The Support Period for FOSCAM components is actively maintained considering security updates from Jan 2022 to Jan 2025.

*This list is constantly being updated and subject to change without notice.

Models	Versions	Description
VD1	V1.0	Video Doorbell
V5P,V5S,V9905P,V9915P	V1.0	Wireless IP Camera
V8P,V8S,V9908P,V9918P	V1.0	Wireless IP Camera
G4C,G5C, G4S, G5S	V1.0	Wireless IP Camera
R8M,R8S,R8C,R8P,L8M	V1.0	Wireless IP Camera
L8M,L8S,L8C	V1.0	Wireless IP Camera
R4M,R4S,R4C.R4P	V5.0	Wireless IP Camera
C5M,C5B,C5D,C5P	V1.0	Wireless IP Camera
C5M,C5B,C5D,C5P	V2.0	Wireless IP Camera
X5,X5P	V6.0	Wireless IP Camera
R5	V6.0	Wireless IP Camera
PD5,PA5,PW5,PS5	V1.0	Wireless IP Camera
D8T,D8A,D8H,D8I	V1.0	Wireless IP Camera
SD8P,SD8, SD8T,SD8V	V1.0	Wireless IP Camera
SD4H,SD4T,SD4P,SD4V	V1.0	Wireless IP Camera
SD4,SZ4,SDZ	V4.0	Wireless IP Camera
D4Z, VZ4,OZ4, W4Z	V5.0	Wireless IP Camera
B4,BG4,B4W,B4C,BS4	V2.0	Battery Security Camera
BP4,BP4W,BP4C	V1.0	Battery Security Camera
FN8108W,FN9108W,FNA108W,FN8108W-B4.FN9108W-B4,FNA108W-B4	V1.0	Wi-Fi Network Video Recorder
FI9911W,FI9910W Pro,FI9911W Pro	V1.0	Wi-Fi Network Video Recorder
FI9925W,FI9935W,FI9945W,FI9925W Pro	V1.0	Wi-Fi Network Video Recorder
V5W,V9905W,V9915W,V9925W	V1.0	Wi-Fi Network Video Recorder