Queensferry House
Carnegie Campus
Enterprise Way
Dunfermline
Fife, KY11 8GR
UK

Purpose

The purpose of this document is to provide guidance to Optos customers on the processes to follow in the event of a suspected cybersecurity or security vulnerability in any Optos product. This document provides Optos customers with all of the necessary information to understand how they can report and receive information on these types of incidents and how Optos handles events of this type.

Policy

This document is Optos Policy on potential and reportable security vulnerabilities. This document includes the process with timelines and responsibilities for all parties involved in the reporting and disclosure of these types of summaries.

Security Incident Receipt and Response

Optos Customer Service and the Customer Service Helpdesk will handle the initial receipt of any potential reported Cybersecurity Incident or Vulnerability. This will be escalated to the Optos Security Incident Response Team (SIRT) for triage and assignment. The SIRT is responsible for responding to potential security and cybersecurity incidents.

The SIRT is a global team that deals with the investigation, and public reporting of potential security vulnerabilities and Cybersecurity issues with Optos products.

Optos definition of a potential cybersecurity vulnerability is:

A potential or identified weakness in the computational logic found in software and hardware components that, when exploited, can result in a compromise in the security of the product, and can lead to denial, delay or breach of the product and service provided.

Optos may deviate from this definition based on the circumstances and outcomes of any investigation of the reported incident.

The SIRT was established in accordance with the standard ISO/IEC 29147:2018, which include the guidelines for disclosure of potential vulnerabilities.

The Optos Customer Helpdesk is available to contact globally (see Contact Us (optos.com) for your regional contact and availability. Optos also work with independent third parties which include; security researchers, consultants, industry organizations, and other vendors to identify possible security vulnerabilities and issues with Optos products.

Queensferry House
Carnegie Campus
Enterprise Way
Dunfermline
Fife, KY11 8GR
UK

Informing Optos of a Potential Security Vulnerability

Anyone suspecting that they are experiencing or may have identified a product security issue is strongly encouraged to contact the Optos Customer Helpdesk. Optos will consider reports from all sources (e.g. third party vendors, research organisations, customers, suppliers) concerned with product or network security and escalate to the SIRT for review.

For general security concerns about Optos products the Optos Customer Support Team can provide the appropriate technical assistance. They can also support non-essential/lower priority software upgrades including any security updates.

To allow us to investigate and respond please provide:

Date of issue, issue description of the potential vulnerability, system/product affected where applicable and Country/Location of report.

To contact the Optos Helpdesk, use one of the following methods (see Contact Us (optos.com) for global contacts):

	Customer Support
Phone	Freephone UK only: 0808 100 4546 USA Toll-free: 800-854-3039 or 833-655-1770
	Nonemergency Support
Email	ics@optos.com
Hours	Support requests that are received via email are typically acknowledged within 48 hours.

Queensferry House
Carnegie Campus
Enterprise Way
Dunfermline
Fife, KY11 8GR
UK

Optos encourages customers to provide any information that can to support any identified security concerns or vulnerabilities identified. Optos will provide a secure area for customers to share information/data that may be helpful in any investigation into cybersecurity issues. Please contact Optos Customer Support directly or through the customer portal to arrange a secure transfer of any information. Optos handles all data as per our Global Privacy Policy, Optos Global Privacy Policy

Publishing of Security Vulnerability Information from Optos

To ensure you are up to date with the latest information, and can receive the latest security vulnerability information from Optos, customers should review the following table and information provided, to determine the appropriate option for them:

optos.com	www.optos.com
Customer Portal	CDP Login (optos.com)
Email	ics@optos.com
Optos Blog	https://www.optos.com/blog/

Optos.com

Optos will provide any major security vulnerability announcements and cybersecurity information on our products via our website on the home page and via out Customer Portal.

Customer/Distributor Portal

All Optos Customers and Distributors should sign up/log in to the relevant portal when purchasing an Optos Device. The portals will provide all information on any available product and supporting document updates periodically. Any security vulnerabilities will be reported to Customers and Distributors through these portals via notifications when the user logs in.

Queensferry House
Carnegie Campus
Enterprise Way
Dunfermline
Fife, KY11 8GR
UK

These notifications will require acknowledgement to ensure that they are read and understood by our users.

Email

Optos Security Advisories provide information about Critical or High severity security vulnerabilities. These will be distributed to the appropriate mailing list per product when they are available. The Optos SIRT may also send Informational advisories to the relevant customer and distributor mailing lists as required. Informational advisories are used not as a disclosure mechanism for any Optos vulnerabilities but for sharing information on security incidents that may impact Optos products and that may be of interest to Optos customers and distributors.

Emails are sent for the initial release and significant updates to Optos Security Advisories. A significant update is advisory content that could result in the customer addressing the vulnerability in a different manner. Examples of a major advisory change include, changes to changes in Security Impact Rating (SIR; see the Assessing Security Risk—Common Vulnerability Scoring System and the Security Impact Rating section of this document), and changes in fix information. Customers that require automated alerts for should subscribe to the Optos blog Really Simple Syndication (RSS) feed or check their Customer Portal for notifications. All Security Advisories will be displayed in chronological order, with the most recent advisories and updates appearing at the top of the page.

Optos Blog/RSS Feed

Anyone can receive updates via Blog (optos.com). Security vulnerability information will be posted to our RSS feeds from Optos.com Blog. This does not require an active Optos.com registration and is available freely. To subscribe to the RSS feeds, visit the Blog (optos.com) site and enter your email address in the “Get Posts in Email” textbox.

Notifying Optos of a Potential Issue

The Optos Customer Portal allows registered Optos users to subscribe to and receive important Optos product and technology information, including Optos Security Notifications. The users can also contact optos directly through this medium and through our customer support address ics@optos.com.

Queensferry House
Carnegie Campus
Enterprise Way
Dunfermline
Fife, KY11 8GR
UK

Public Relations or Press Queries Regarding Optos Security Vulnerability Information

The following table shows the Optos press contacts for Optos security vulnerability information.

	Press Contacts
Who?	Optos Media Relations/Marketing
Additional Public Relations	mediarelations@optos.com

Commitment to Product Security/Integrity

Optos development policies and procedures prohibit any intentional behaviours or product features that are designed to allow unauthorized device or network access, and may lead to an exposure of sensitive information, or a bypass of security restrictions or features.

Optos will investigate any report of potential issues of this nature with the highest priority and actively encourage all parties to report potential vulnerabilities to the Optos Customer Support Helpdesk. All reports of these vulnerabilities will be managed, addressed and disclosed in accordance with the terms of this Policy.

Queensferry House
Carnegie Campus
Enterprise Way
Dunfermline
Fife, KY11 8GR
UK

Optos Product Security Incident Response Process

Figure 1 illustrates the vulnerability life cycle and the Optos SIRT disclosure and resolution process at a high level.

Figure 1. Optos Product Security Incident Response Process

The steps in the process illustrated in Figure 1 are as follows:

1. **Notification:** SIRT receives notification of a security incident.
2. **Assign:** SIRT categorise, prioritises and identifies resources to investigate.
3. **Assess and Action:** SIRT coordinates the impact assessment across all products and fixes where appropriate.
4. **Report:** SIRT ensures the incident is reported to Customers, Vendors and appropriate authorities where this is deemed a requirement in response to the reported security vulnerability.

Queensferry House
Carnegie Campus
Enterprise Way
Dunfermline
Fife, KY11 8GR
UK

1. When Optos are notified or become aware of any security incident it will be escalated to the SIRT. The Optos SIRT will investigate all reports pertinent to all products that may be affected, unless the product is end of life.
2. The Optos SIRT will assign a risk category as per process and determine the priority of the reported incident. If necessary, the SIRT will collaborate with the reporting entity to ensure we have all of the required information, understand the details of the vulnerability, and determine the appropriate actions where required.
3. During the investigation, the Optos SIRT will determine the impact of the incident on all products and provide the results of the investigation to the reporting entity. If a fix is required, the timeline for this will be communicated, along with an action plan for resolution. If there is any concerns raised Optos will discuss these with the reporting entity to try and resolve any issues.
4. Optos SIRT will ensure that the incident is reported appropriately, including any cases where wider public disclosure is required or in the case that the relevant authorities may require notification.

The Optos SIRT will ensure that all sensitive information or Personally Identifiable Information will be handled on a highly confidential basis and in compliance with regulations such as HIPAA, GDPR etc. All Optos employees that handle this manner of incidents are trained on our Global Data Handling Policies and Procedures and distribution will only include individuals who have a legitimate need to know and can actively assist in the resolution. Optos recommend that the reporting entity also maintain strict confidentiality until complete resolutions are available for customers and have been published by the Optos SIRT on the Optos website through the appropriate coordinated disclosure.

Optos will not use any of your data or identity in the public disclosure unless permission has been given by the reporting entity or entities involved.

The Optos SIRT may use third-party vendors to assist with investigation, technical/legal support and notification of security vulnerabilities. In the case of a third-party requiring access to sensitive data, Optos will seek permission from the parties affected.

If a reported vulnerability involves a vendor product, the Optos SIRT will notify the vendor directly, coordinate with the incident reporter and ensure the response process is followed to conclusion.

The Optos SIRT will coordinate with the reporting entity to ensure that updates and information is provided in a timely manner and that the progress of the incident is understood.

Queensferry House
Carnegie Campus
Enterprise Way
Dunfermline
Fife, KY11 8GR
UK

If during the investigation of the report it is determined that the incident does not affect a Optos product but does involve another vendor's product, Optos will report the matter to the parties affected and determine the next steps with the reporting entity to ensure the matter can be concluded appropriately.

Any resolution of a reported incident may require upgrades to products that are under active support from Optos. Optos strongly recommends that customers periodically ensure that they have the latest software updates and check the Optos Customer Portal regularly for available updates.

Security Vulnerability Disclosure Discovered By Other Means

In the course of undertaking normal business activities, if Optos become aware of a new or previously unidentified security vulnerability, Optos will follow the Process Outlined in this Policy. All Vulnerabilities found in Optos products will be subject to the same processes and handled by the Optos SIRT. If the vulnerability is identified in a third-party product, Optos will report this to the third party directly, unless the affected customer wishes to report the vulnerability to the vendor directly; in that case, Optos will facilitate contact between the customer and the vendor and ensure the matter is dealt with in accordance to this policy.

Optos will handle all personal data as per its privacy notice and ensure confidentiality is maintained. Optos will not share any customer-specific data unless directed to do so by the affected customer, or as required by a legal investigation.

Assessing Security Risk—Common Vulnerability Scoring System and the Security Impact Rating

Optos uses Version 3.1 of the Common Vulnerability Scoring System (CVSS) as part of its standard process of evaluating reported potential vulnerabilities in Optos products. The CVSS model uses three distinct measurements, or scores, that include Base, Temporal, and Environmental calculations. Optos will provide an evaluation of the Base vulnerability score. Optos will calculate the Environmental score based on the standard system installation configuration. The combination of all three scores should be considered the final score, which represents a moment in time and is tailored to a specific environment. Organizations are advised to use this final score to prioritize responses in their own environments.

In addition to CVSS scores, Optos uses the Security Impact Rating (SIR) as a way to categorize vulnerability severity in a simpler manner. The SIR is based on the CVSS

Queensferry House
Carnegie Campus
Enterprise Way
Dunfermline
Fife, KY11 8GR
UK

Qualitative Severity Rating Scale of the Base score, may be adjusted by SIRT to account for Optos-specific variables, and is included in every Optos Security Advisory. Optos uses the following guidelines to determine the Optos Security Advisory type. Security Advisories for Critical and High include fixed software information.

Type	CVSS	CVE	Fix Information
Critical	9.0–10.0	Yes	Fix information in the Security Advisory and bug. Detailed fix information for Optos Software can be obtained in the release notes.
High	7.0–8.9	Yes	Fix information in the Security Advisory and bug. Detailed fix information for Optos Software can be obtained in the release notes.
Medium	4.0–6.9	No	If any workaround required, this will be detailed in a bulletin or release notes. Fix information in bug (if applicable).
Low/Informational	N/A	No	Fix information in bug (if applicable).

Issues with a Medium or Low SIR are only published in the software release notes if any risk is considered a threat or a workaround is required. These are not published as part of a Security Advisory.

Optos reserves the right to deviate from these guidelines in specific cases if additional factors are not properly captured in the CVSS score.

Queensferry House
Carnegie Campus
Enterprise Way
Dunfermline
Fife, KY11 8GR
UK

If there is a security issue with a third-party software component that is used in a Optos product, Optos typically uses the CVSS score provided by the third party. In some cases, Optos may adjust the CVSS score to reflect the impact to the Optos product.

Third-Party Software Vulnerabilities

If there is a vulnerability in a third-party software component that is used in a Optos product, Optos typically uses the CVSS score detailed above. Optos may adjust the CVSS score to reflect the impact to Optos products.

Optos will consider a third-party vulnerability "high profile" if it meets the following criteria:

- The vulnerability exists in a third-party component.
- Multiple Optos products are affected.
- The CVSS score is 5.0 or above.
- The vulnerability has gathered significant public attention.
- The vulnerability is likely to have exploits available and is expected to be, or is being, actively exploited.

For high profile, third-party vulnerabilities, Optos will begin assessing all potentially impacted products and publish a Security Advisory within 24 hours after Optos classifies the vulnerability as high profile. All known affected Optos products will be detailed in an update to the initial Security Advisory that will be published within 7 days of the initial disclosure. The security advisory will include each vulnerable product so that registered customers can view them using the Optos Customer Portal. Any vulnerabilities that are not classified as high profile will be disclosed in a Release Note.

Optos Incident Reporting/Management History

All vulnerability reports received by Optos will be maintained in our CRM System Database. Any Security Incidents that have a High or Medium severity assigned will have an associated JIRA issue number assigned and subsequently retained for the lifetime of our devices, plus two years. A history of all the releases related to security vulnerabilities will be maintained on our website/customer portal.

Customers may request a Vulnerability Report for any Optos Product. Optos will provide information for the customer from our customer relations management systems and supporting security vulnerability identification systems. These should also be available to the customer on the software release notes where appropriate.

Queensferry House
Carnegie Campus
Enterprise Way
Dunfermline
Fife, KY11 8GR
UK

These will include any Vulnerabilities found in the Cybersecurity and Infrastructure Security Agency (CISA)'s Known Exploited Vulnerabilities (KEV) Catalog and Vulnerabilities that Optos has determined to be high-risk.

Security Notifications

Optos will provide all information necessary to inform the user with of potential steps needed to protect their environment. Optos will not expose any vulnerability details that could be exploited. Please ensure you have subscribed to the relevant links provided to stay current with all published Vulnerability Reports and are not using historic information.

Optos will provide security-related releases on the Optos Customer/Distributor Portals and on optos.com.

Security Advisory Action

Optos will provide detailed information about security issues that directly involve Optos products and require an upgrade, fix, or other customer action. Security Advisories are used to disclose vulnerabilities with a Critical, High, or Medium SIR. The Optos SIRT only validates the affected and fixed version information documented in the advisory.

Advisories are normally published if a third party or Customer makes a public statement about a Optos product vulnerability and may also be used to proactively notify customers about a security-related issue that is not a vulnerability.

Advisory Responses

Optos Advisory Responses will provide customers and affected parties with information about security events that have the potential for widespread impact on customer networks, applications, and devices. Optos Event Responses contain summary information, threat analysis, and mitigation techniques that feature Optos products and cloud-hosted services. They are normally published under the following circumstances:

- If a significant security vulnerability exists in a vendor's product that could affect a Optos product due to interoperation with the vendor's product or use of the network as a vector for exploitation
- In response to the release of Optos IOS and IOS XE, Optos IOS XR, Optos NX-OS, and Optos ASA, FTD, and FMC Software bundled publications

Queensferry House
Carnegie Campus
Enterprise Way
Dunfermline
Fife, KY11 8GR
UK

Release Notes

Release Notes are used to disclose issues with a Low or Medium SIR. All Optos bug IDs that are disclosed by Optos are available for registered customers to view in the Release Notes provided with your software.

If a Optos Security Advisory references a bug, the bug entry in the Release Notes will link to the relevant Optos Security Advisory.

Any Optos bug that has been evaluated by the Optos SIRT will include a "SIRT Evaluation" section in its supporting Security Advisory. This section includes the CVSS score and severity where appropriate. Customers are invited to use this additional information at their discretion and correlate Optos bugs with industry events.

Customers who wish to upgrade to a software version that includes fixes for those issues should contact their normal support channels. Any exception to this policy will be determined solely at the discretion of Optos.

Public Notifications

Optos will publicly disclose Optos Security Advisories if:

- The Optos SIRT the incident has been fully investigated, the process is complete and Optos has determined that the vulnerability can be addressed sufficiently through available means (patches, workarounds, etc.), or a process/software release is in place to sufficiently address the issue.
- An active or potential increased risk of exploitation of a vulnerability has been identified or uncovered by The Optos SIRT which could culminate in increased risk for Optos customers. Optos will expedite any notification in this instance ensuring the vulnerability can be addressed with a patches or workaround.

Optos publications will be available via all platforms described in this policy and may be specified by individual product including notifications to the public and third parties.

Optos reserves the right to deviate from this policy on an exception basis to ensure access to Optos.com for software patch availability.

Queensferry House
Carnegie Campus
Enterprise Way
Dunfermline
Fife, KY11 8GR
UK

Notification Schedule

Optos will release Optos Security Advisories when required via the platforms described in this policy. We will endeavour to a schedule an update for customers annually via these platforms. This schedule applies to the disclosure of vulnerabilities in the Optos products and does not apply to the disclosure of vulnerabilities in third party products.

Incident Response Support

All customers, regardless of contract status, are eligible for support from the Optos Customer Support Helpdesk for a known or investigable vulnerability in Optos products. Please contact Optos at the addresses provided in the contact section of www.optos.com with details of the vulnerability to allow us to respond as per this policy.

Optos reserves the right to determine the type and degree of free assistance it may offer in connection with any incident and to withdraw from such an incident at any time. The assistance you are eligible for will be defined in your terms and conditions of your contract.

Security Software Updates

Optos customers with service contracts should obtain updates for security fixes through their usual support channels, these will generally be available in the Customer or Distributor Portal, Via notification on your device or by contacting the Customer Support Helpdesk Directly. Optos recommends contacting the Customer Support Helpdesk only with specific and imminent problems or questions.

If you are without a service contract or it has expired, please contact Optos to discuss the best method of support for your issue. Optos may provide security updates for known vulnerabilities free of charge in cases where a High or Critical potential vulnerability has been identified.

Software Release Terms and Conventions

Maintenance Releases

Optos has a fixed internal release schedule for each of its products and supporting software. Maintenance releases are generally driven by external factors such as customer feedback or issues reported through customer service and are prioritised through our internal review processes.

Queensferry House
Carnegie Campus
Enterprise Way
Dunfermline
Fife, KY11 8GR
UK

Optos intend to meet scheduled dates per platform as best as we can and where appropriate make aware through customer service. We reserve the right to adjust the schedule based on priorities, and other external factors which may influence the release dates published.

For information on scheduled releases, please contact Optos customer service if there are any questions or concerns with regards to the maintenance of your software or device configuration. Optos will provide any information necessary to ensure that your configuration is as secure as possible. In the event of a specific cybersecurity vulnerability issue, please follow the procedures outlined in this policy.

Prioritisation based on external factors (acceleration)

Hot Fix Availability

Optos can make "Hot Fixes" available where the need for a response or solution to a reported event or scenario is necessary. Optos adopt a risk-based approach based on outcome of investigation (CVSS score) of the issues we have identified or been notified as part of this policy.

Optos goal is to respond within one week period (within 5 business days) of confirmation that a hot fix is necessary to address a cybersecurity vulnerability. This will be influenced by several factors, including test results, threat identification, verification of the influencing factors and available mitigations or workarounds.

All issues are managed on case-by-case basis dependant of risk and when identifies will be detailed in the release notes of the software or communicated directly to the affected parties or product base.

OS Patches

Optos will communicate with customers if the OS requires to be updated on their devices. In the instance of a required security update, this will be either directly communicated to our customers, or managed through our customer portal. Our customer support team will assist if necessary to ensure that your device can be brought up to date with the latest OS security updates where appropriate. The image server which supports the device has auto update enabled and Optos recommend that the software is kept up to date weekly and updates are checked on a weekly basis by the customer or their IT support team.

Last Updated: 2024 February 16