Agfa Radiology Solutions
Global Policy
Vulnerability Disclosure

Changes compared to the previous published version are identified with a red line in the margin and documented in the revision history

Content

1. Scope

This Global Vulnerability Disclosure Policy is applicable to the Agfa Radiology Solutions Division (hereafter referred to as Agfa RSD or RSD) global organization and its products with the ability to connect to a network, which are not End of Service Life.
All other products shall be out of scope.

2. Purpose

Products with Information Security & Privacy (ISP) vulnerabilities undermine our customers' ability to protect information security and privacy.
Agfa Radiology Solutions is committed to resolving vulnerabilities to meet the needs of its customers and the broader technology community.
This document describes Agfa RSD's policy for receiving reports related to potential information security and privacy vulnerabilities in its products and the company's standard practice with regards to informing customers of verified vulnerabilities.

3. Policy

3.1. Policy Statement

Anyone must be able to report potential information security and privacy vulnerabilities identified in any Agfa RSD products with the ability to connect to a network.

3.2. Reporting a Vulnerability

3.2.1. When and How to Contact Agfa RSD

Contact Agfa RSD when you have identified a potential security vulnerability with one of our products.
This can be done by:

1. Filling out the information requested in the Agfa RSD Vulnerability Reporting Form
    - Alternatively, you can scan the following QR code:

2. Submitting the form

Agfa RSD requests the reporter keep any communication regarding the potential security vulnerability confidential.

3.2.2. Follow-up

After the potential security vulnerability report is received, the appropriate personnel will contact the reporter to follow-up.
Agfa RSD attempts to acknowledge receipt to all submitted reports within fourteen days.

If Agfa RSD determines that the reporter has not provided enough information, the reporter may be requested to provide additional details.

If necessary, Agfa RSD shall communicate with other vendors in its supply chain.

Status updates will be provided to the reporter via the same communication channel which was used to submit the potential security vulnerability report. The rate at which status updates are provided may vary.

3.2.3. Credit

Should reporters choose to be recognized for their efforts, they shall be mentioned in the released security advisories.

3.3. Receiving Security Information from Agfa RSD

In most cases, Agfa RSD will issue a security advisory when a practical workaround or fix for the particular security vulnerability has been identified.
As each security vulnerability case is different, Agfa RSD can take alternative actions in connection with issuing security advisories.
Agfa RSD can determine to accelerate or delay the release of an advisory or not issue one at all.

Agfa RSD does not guarantee that security advisories will be issued for any or all security issues customers can consider significant or that advisories will be issued on any specific timetable.

Technical security information about our products and services is distributed through several channels:

a) Agfa RSD distributes information to customers about security vulnerabilities via the Agfa RSD ISP Communications mailing list. You can subscribe here.
   - Alternatively, you can scan the following QR code:

b) Security-related information can also be distributed by Agfa RSD to public newsgroups or electronic mailing lists. This is done on an ad hoc basis, depending on how Agfa RSD perceives the relevance of each advisory to each forum.

All aspects of this process are subject to change without notice, as well as to case-by-case exceptions. No level of response is guaranteed for any specific issue or class of issues.

3.4. Applicable Standards

Agfa RSD's Vulnerability Handling & Disclosure processes shall be in line with:

- ISO/IEC 29147:2018
- ISO/IEC 30111:2019

4. References

References

Doc ID / Location	Title
Office 365	Agfa RSD Vulnerability Reporting Form
Office 365	Agfa RSD ISP Communications mailing list

5. Revision History

Version #	Author	Change	Training Need
1-2	BPM ISP	Initial version	No (target audience is external)

AGFA

Details as of PDF Creation Date

Document Metadata

Title:	Global Policy RSD - Vulnerability Disclosure.docx
Livelink ID:	83736298
Version#:	2
Version Date:	2024-09-12 02:42 PM CET
Status:	Approved on 2024-10-30 03:53 PM CET
Owner:	Eurico Silva Maia (apypv)
Created By:	Eurico Silva Maia (apypv)
Created Date:	2024-07-30 02:00 PM CET
PDF Creation Date:	2025-02-07 08:10 AM CET

This document was approved by:

Signatures:

1. Koen Vervoort (awpze) on 2024-10-30 03:32 PM CET
2. Toon Brynaert (axebw) on 2024-10-24 08:23 PM CET
3. Eurico Silva Maia (apypv) on 2024-10-24 01:11 PM CET

Detailed Approver History:

- **Approval Workflow started on 2024-10-24 01:07 PM CET**
  - Approval task originally assigned to and completed by Toon Brynaert (axebw) on 2024-10-24 08:23 PM CET
  - Approval task originally assigned to and completed by Koen Vervoort (awpze) on 2024-10-30 03:32 PM CET
  - Approval task originally assigned to and completed by Eurico Silva Maia (apypv) on 2024-10-24 01:11 PM CET

Version & Status History

Version#	Date Created	Status
2	2024-09-12 02:42 PM CET	Approved - 2024-10-30 Reviewed - 2024-09-26
1	2024-07-30 02:00 PM CET	

Applied Categories and Attributes:

IMS RSD	
Effective Date:	02/07/2025
Review Date:	02/07/2027
IMS Editor:	Ivan Peeters (ambth)

Document Owner:	Eurico Silva Maia (apypv)
Doc Type:	Policy
Org Level:	Agfa Radiology Solutions -> Agfa Radiology Solutions
Process:	Information Security & Privacy -> Information Security & Privacy
Site:	All
Global Process Roll Out:	