

Notification de sécurité produit URGENTE

Risque de discordance des données pendant le protocole de transfert de fichiers (FTP) pour le système Essenta DR Compact

Septembre 2023

Ce document contient des informations importantes pour assurer le bon fonctionnement continu et en toute sécurité de votre matériel.

Veuillez examiner les informations suivantes avec tous les membres de votre personnel qui doivent en avoir connaissance. Il est important d'en comprendre les conséquences.

Veuillez conserver ce courrier dans vos dossiers.

Madame, Monsieur,

Philips a identifié un problème potentiel de cybersécurité avec les systèmes Essenta DR Compact, qui pourrait entraîner la divulgation ou la modification non autorisée des données patient. Cette Notification de sécurité produit URGENTE est destinée à vous informer des points suivants :

1. La nature du problème et les circonstances dans lesquelles il peut survenir ;

Il existe un problème potentiel de cybersécurité avec les systèmes Essenta DR Compact, qui pourrait entraîner la divulgation ou la modification non autorisée des données des patients. Ce problème peut survenir si un pare-feu n'est pas en place, si le protocole de transfert de fichiers (FTP) est utilisé et si la séquence d'événements suivante se produit :

- Le personnel non autorisé bénéficie d'un accès physique à votre établissement
- Votre établissement ne dispose pas d'un pare-feu et/ou d'une séparation réseau pour isoler les dispositifs médicaux, et
- La personne non autorisée connecte son appareil au réseau du système Essenta DR Compact au moment précis où les données sont transférées (les données ne sont pas transférées en continu).

Dans ces conditions, l'accès ou la modification non autorisés des données patient est possible.

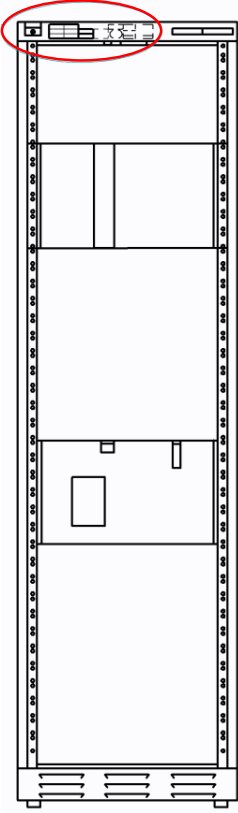
2. Risque/danger associé au problème

En cas d'accès non autorisé, le risque pour les utilisateurs et les patients inclut le risque de mélanger les images et/ou les noms des patients, ce qui entraîne une erreur de diagnostic. Le problème peut également nécessiter de réaliser une nouvelle acquisition du patient.

3. Systèmes concernés et identification de ces derniers

Identification des systèmes concernés :

Tous les systèmes Essenta DR Compact sont concernés. Les systèmes peuvent être identifiés par le nom du modèle, qui se trouve sur l'étiquette du système (voir les cases rouges dans la Figure 1).

Exemple d'étiquette du système Essenta DR Compact	Emplacement de l'étiquette (Générateur de l'armoire du système)	Modèle	Numéro de référence (REF)
 PHILIPS type 9890-010-8738. SNwkkxxxx Essenta DR Class I - TYPE B IEC 60601-1 Associated equipment IEC 60601-2-32:1994		Système Essenta DR Compact	712072

Utilisation prévue :

Le système Essenta DR est un système de radiologie numérique multifonction, adapté à tous les examens radiographiques de routine, y compris les domaines spécialisés tels que la traumatologie ou la pédiatrie, à l'exception de la mammographie.

Il est conçu pour la radiographie d'un patient debout, assis ou allongé, en combinaison avec une table de radiographie mobile (chariot).

Le système est conçu pour l'imagerie numérique directe à l'aide du capteur-plan intégré et, en outre, aux acquisitions libres sur cassettes radiographiques.

4. Actions que le client/utilisateur doit mettre en œuvre afin de prévenir tout risque pour les patients ou les utilisateurs

- Installez un pare-feu pour assurer une communication sécurisée lors de l'utilisation du FTP pour transférer des données. Philips déconseille l'utilisation du système sans pare-feu.
- Reportez-vous à l'annexe A pour connaître les recommandations en matière de protection du réseau et joignez cette notification en tant qu'addenda au Manuel d'utilisation du système Essenta DR Compact fourni avec le système pour pouvoir vous y référer ultérieurement.

- Transmettez cette notification à tous les utilisateurs de cet appareil et à votre service de sécurité informatique afin qu'ils soient au courant du problème.
- Les clients peuvent continuer à utiliser les systèmes concernés conformément à leur utilisation prévue.
- Veuillez remplir et renvoyer le formulaire de réponse ci-joint à Philips dans les plus brefs délais et au plus tard dans les 30 jours à compter de sa réception. En remplissant ce formulaire, vous confirmez avoir reçu la Notification de sécurité produit et compris le problème ainsi que les actions à mettre en œuvre.

5. Actions prévues par Philips pour remédier à ce problème

Philips fournit cette Notification de sécurité produit qui contient des recommandations pour la protection du réseau décrites dans l'Annexe A.

Soyez assuré que notre priorité est de maintenir un niveau élevé de sécurité et de qualité. Pour toute information complémentaire ou demande d'assistance technique concernant ce problème, veuillez contacter votre représentant Philips :

0800 80 3001

Philips vous présente toutes ses excuses pour la gêne occasionnée par ce problème.

Nous vous adressons, Madame, Monsieur, nos sincères salutations.

Karmen Greunert
Responsable qualité Radiologie diagnostique (DXR)

Formulaire de réponse à la Notification de sécurité produit URGENTE

Référence : vulnérabilité de sécurité du FTP du système Essenta DR Compact (2023-PD-DXR-009)

Instructions : veuillez remplir et renvoyer ce formulaire à Philips dans les plus brefs délais et au plus tard 30 jours à compter de sa réception. En remplissant ce formulaire, vous confirmez avoir reçu la Notification de sécurité produit URGENTE et compris le problème ainsi que les actions à mettre en œuvre.

Nom du client/du destinataire/de l'établissement : _____

Adresse postale: _____

Ville/Département/Code postal/Pays : _____

Actions à mettre en œuvre par le client :

Suivez les instructions fournies à la section 4 et l'annexe A de cette Notification de sécurité produit URGENTE.

Nous accusons réception de la Notification de sécurité produit URGENTE ci-jointe, reconnaissons avoir compris cette dernière et confirmons que les informations contenues dans cette notification ont été transmises de manière appropriée à tous les utilisateurs qui manipulent les systèmes concernés.

Nom de la personne qui remplit le présent formulaire :

Signature : _____

Nom (en majuscules) : _____

Fonction : _____

Numéro de téléphone : _____

Adresse électronique : _____

Date
(JJ/MM/AAAA) : _____

Veuillez remplir le formulaire de réponse et le renvoyer à Philips par e-mail dans les plus brefs délais et au plus tard 30 jours à compter de sa réception à l'adresse suivante :

dach.cs.pmplanning.gbs@philips.com

Annexe A : addenda au manuel d'utilisation du système Essenta DR Compact

Pare-feu

Un pare-feu correctement configuré peut contribuer à réduire le risque de vulnérabilité via le réseau. Un pare-feu est conçu pour bloquer les accès non autorisés au réseau tout en permettant les communications autorisées. Philips déconseille l'utilisation du système sans pare-feu. En outre, il est recommandé d'attribuer le système à un segment de réseau séparé, par exemple, un VLAN séparé pour les dispositifs médicaux.

Les systèmes basés sur Eleva exécutent un pare-feu préconfiguré intégré. Les systèmes peuvent être commandés avec et sans pare-feu (matériel) externe. Le pare-feu est configuré lors de l'installation du système via l'application de service Philips.

Les utilisateurs qui ont des questions concernant leur solution spécifique de systèmes Essenta DR Compact Philips sont invités à contacter leur équipe de support technique Philips locale ou l'assistance technique régionale. Les coordonnées de Philips sont disponibles à l'adresse suivante.

<https://www.philips.com/productsecurity>

Si l'hôpital choisit d'installer son propre pare-feu, la liste de ports ci-dessous doit être configurée.

Port	Transport Layer Protocol	Fixed	Inbound	OutBound	Usage
3010	TCP	No	Y	N	DICOM
80, 4440	TCP	Yes	Y		Remote Service FSF for AWS
5900	TCP	Yes	Y		Remote Service via VNC for AWS
17991	TCP	Yes	Y		legacy Fuji control protocol which replaces the RS232 control line
18015 - 18020, 18030, 18050	TCP	Yes	Y		PCR Reader Integration
21	TCP	Yes	Y		FTP for PCR Reader integration
50123	TCP	Yes	Y		Remote Service: CDF Provider Server (for Logserver)
80	TCP	Yes		Y	VirusGuard Updates (EPO / distribution server / http)
443, 8086, 9006, 9900	TCP	Yes		Y	Remote service.
5104	TCP	No		Y	To RIS
6104	TCP	No		Y	To PACS
104	TCP	No		Y	To Printer
445	TCP	Yes		Y	DosePRN_445
9100	TCP	Yes		Y	DosePRN_JETDIRECT
515	TCP	Yes		Y	DosePRN_LPR
137 - 139	TCP&UDP	Yes		Y	DosePRN_SYSCO
123	UDP	Yes		Y	Time Synchronization
514	UDP	No		Y	Audit Trial
80, 104, 443, 6464	TCP	Yes		Y	iSite
>1023	TCP	Yes		Y	FTP RIS
514	UDP	No		Y	Dicom Print
80, 23	TCP	Yes		Y	PCR READER_CONF
18018	TCP	Yes		Y	PCR READER_FRUP
>1023	TCP	Yes		Y	PCR READER_FTPDATA