BD is aware of a Trojan called Kwampirs, which allows malicious attackers remote access into a compromised computer. **This is not a BD-specific vulnerability and there have been no reports of a BD product being affected by Kwampirs**. It has been observed targeting common legacy Microsoft Windows operating systems. Kwampirs affects those systems with enabled network shared drives, outdated or no malware protection and any Windows Operating System.

Products in Scope

BD has provided a list of products in scope that use Microsoft Windows operating system that is potentially vulnerable to Kwampirs in order to help our customers prioritize remediation steps given the severity level assigned to each BD product. BD uses the Common Vulnerability Scoring System v3.0 (CVSS) for this purpose and rate the characteristics of a vulnerability and produce a base numerical score reflecting the severity.

Important: BD has confirmed anti-virus software is up to date for products in scope where BD maintains an anti-virus solution. If you have a BD product, where BD maintains an anti-virus solution, there is no customer action needed. Customers that maintain anti-virus independent of BD automated updates should ensure they follow the actions outlined under mitigation and compensating controls in the bulletin.

Product Name(s)	CVSS Score	CVSS Rationale
BD Alaris™ Gateway Workstation*	Medium - 4.8	CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N Hospital network access and compromise is required for the malware to affect the device. Attack complexity is high because an attacker would have to compromise a hospital network in order for the Kwampirs attack to become successful. Attack complexity is high based on successful hospital's network infiltration and vulnerable enabled network shares are found to further propagate. Privileges to authenticate to the shared drives on a customer network are required by default unless modified by the customer. The malware does not require user interaction to spread from device to device once the initial infection takes place. The scope is considered unchanged as the malware is shared from the connected share to the attached device. The impact is high based on the confidentiality of the data stored on the system or network attached shares.
BD Pyxis Logistics*		
BD Pyxis™ IV Prep*	Medium - 4.2	CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N Hospital network access and compromise is required for the malware to affect the device. Attack complexity is high because an attacker would have to compromise a hospital network in order for the Kwampirs attack to become successful. Attack complexity is high based on successful hospital's network infiltration and vulnerable enabled network shares are found to further propagate. The privileges on the system are assumed to only allow administrative access, since
Rowa™ Dose*		
Rowa™ vMax*		
BD Pyxis™ Anesthesia 4000 System (WinXP)		

BD Pyxis™ Anesthesia ES System		authentication to the shares are required by default unless modified by the institution. The malware does not require user interaction to spread from device to device once the initial infection takes place. The scope is considered unchanged as the malware is shared from the connected share to the attached device. The impact is high based on the confidentiality of the data stored on the system or network attached shares.
BD Pyxis™ Anesthesia System 4000 (Win7)		
BD Pyxis™ Anesthesia System 4000 (WinXP)		
BD Pyxis™ CathRack v9		
BD Pyxis™ CIISafe 7.0 (WinXP)		
BD Pyxis™ CIISafe 7.1 (Win7)		
BD Pyxis™ CIISafe 8.x (Win7)		
BD Pyxis™ Connect v3.1.x		
BD Pyxis™ CUBIE Replenishment Station (Win7)		
BD Pyxis™ MedStation 3500 (Win7)		
BD Pyxis™ Order Viewer		
BD Pyxis™ Anesthesia ES v1.3. System		
BD Pyxis™ MedStation 4000 Station (Win7)		
BD Pyxis™ MedStation 4000 Station (WinXP)		

BD Pyxis™ MedStation ES v.1.5 BD Pyxis™ MedStation ES v1.3 Pyxis MedStation ES v1.4. System		
BD Pyxis SupplyStation with Kanban BD Pyxis SupplyStation with RFID BD Pyxis™ ScrubStation System	Low - 3.0	CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N Hospital network access and compromise is required for the malware to affect the device. Attack complexity is high because an attacker would have to compromise a hospital network in order for the Kwampirs attack to become successful. Attack complexity is high based on successful hospital's network infiltration and vulnerable enabled network shares are found to further propagate. Privileges to authenticate to the shared drives on a customer network are required by default unless modified by the customer. The malware does not require user interaction to spread from device to device once the initial infection takes place. The scope is considered changed as the malware leverages the shares available on the product to further propagate across the network. The impact is low based on the confidentiality of the data stored on the system or network attached shares.
BD Pyxis™ EcoStation System*	Low - 2.0	CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N Hospital network access and compromise is required for the malware to affect the device. Attack complexity is high because an attacker would have to compromise a hospital network in order for the Kwampirs attack to become successful. Attack complexity is high based on successful hospital's network infiltration and vulnerable enabled network shares are found to further propagate. The privileges on the system are assumed, since administrative authentication to the shares are required by default unless modified by the institution. The malware does not require user interaction to spread from device to device once the initial infection takes place. The scope is considered unchanged as the malware is shared from the connected share to the attached device. The impact is low based on the confidentiality of the data stored on the system or network attached shares.
Alaris Systems Manager BD Alaris™ Connectivity Engine (ACE)	Medium - 4.2	CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N Hospital network access and compromise is required for the malware to affect the device. Attack complexity is high because an attacker would have to compromise a hospital network in order for the Kwampirs attack to become successful. Attack complexity is high based on successful hospital's network infiltration and vulnerable enabled network shares are found to further propagate. The privileges on the system are assumed to only allow administrative access, since authentication to the shares are required by default unless modified by the institution. The malware does not require user interaction to spread from device to device once the initial infection takes place. The scope is considered unchanged as the malware is shared from the

		connected share to the attached device. The impact is high based on the confidentiality of the data stored on the system or network attached shares.
BD Alaris™ Infusion Viewer Suite*	Low - 2.3	CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N Isolated network access and compromise is required for the malware to affect the product. Attack complexity is high based on successful hospital's network infiltration and vulnerable enabled network shares are found to further propagate. The privileges on the system are assumed, since authentication to the shares are required by default unless modified by the institution. The malware does not require user interaction to spread from device to device once the initial infection takes place. The scope is considered unchanged as the malware is shared from the connected share to the attached device. The impact is low based on the confidentiality of the data stored on the system or network attached shares.
FACSCanto II IVD (Canto II / Canto 10C)*	Medium - 4.5	CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N Isolated network access and compromise is required for the malware to affect the product Attack complexity is high based on successful hospital's network infiltration and vulnerable enabled network shares are found to further propagate. The privileges on the system are assumed, since authentication to the shares are required by default unless modified by the institution. The malware does not require user interaction to spread from device to device once the initial infection takes place. The scope is considered unchanged as the malware is shared from the connected share to the attached device. The impact is high based on the confidentiality of the data stored on the system or network attached shares.
BD FACSLyric™ IVD w FACSuite*		
BDFACSVia™ system*		
Accuri C6 Plus (GenIV not Gen II)	Low - 2.3	CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N Isolated network access and compromise is required for the malware to affect the product. Attack complexity is high based on successful hospital's network infiltration and vulnerable enabled network shares are found to further propagate. The privileges on the system are assumed, since authentication to the shares are required by default unless modified by the institution. The malware does not require user interaction to spread from device to device once the initial infection takes place. The scope is considered unchanged as the malware is shared from the connected share to the attached device. The impact is low based on the confidentiality of the data stored on the system or network attached shares.
FACSCanto II RUO w FACSDiva (Canto II / Canto 10C)		
FACSCelesta RUO w FACSDiva		
FACSJazz		
FACSLyric RUO w FACSuite		
FACSVerse w FACSuite		
FACSymphony		
Influx (Sortware)		

LSR Fortessa w FASCDiva (LSR II / LSRFortessa)		
BD EpiCenter™*	Low - 2.6	CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N Isolated network access and compromise is required for the malware to affect the product Attack complexity is high based on successful hospital's network infiltration and vulnerable enabled network shares are found to further propagate. The privileges on the system are assumed, since authentication to the shares are required by default unless modified by the institution. The malware does not require user interaction to spread from device to device once the initial infection takes place. The scope is considered changed as the malware leverages the shares available on the product to further propagate across the network. The impact is low based on the confidentiality of the data stored on the system or network attached shares.
BD Kiestra™ InoqulA*		
BD Kiestra™ TLA / WCA*		
FocalPoint Guided Screen System*		
BD Pyxis™ Connect*	Low - 3.0	CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N Hospital network access and compromise is required for the malware to affect the device. Attack complexity is high because an attacker would have to compromise a hospital network in order for the Kwampirs attack to become successful. Attack complexity is high based on successful hospital's network infiltration and vulnerable enabled network shares are found to further propagate. Privileges to authenticate to the shared drives on a customer network are required by default unless modified by the customer. The malware does not require user interaction to spread from device to device once the initial infection takes place. The scope is considered changed as the malware leverages the shares available on the product to further propagate across the network. The impact is low based on the confidentiality of the data stored on the system or network attached shares.
IDM (Identity Management) *		
MedView Dashboard*		
Patient Association Application*		
Tissue Implant Module (TIMS)*		
Specimen Collection Verification*		
BD Care Coordination Engine		

*These products were not provided with an antivirus solution. Please follow internal best practices to ensure your chosen AV solution is up-to-date to prevent Kwampirs from infecting your environment.