



Medical Devices: Passwords To Pwnage

Scott Erven

Who I Am

Scott Erven



Associate Director – Medical Device & Healthcare Security



Security Researcher



***Over 15 Years Experience and 5 Years Direct Experience
Managing Security In Healthcare Systems***



Over 3 Years Researching Medical Device Security

@scotterven

Agenda

Why Research Medical Devices

Phase 1 Research: Device Vulnerabilities

Phase 2 Research: Internet Exposure

Phase 3 Research: Admin Access

Is AppSec A Problem?

Diagnosis

Treatment Plans



Why Research Medical Devices

Personal Impact

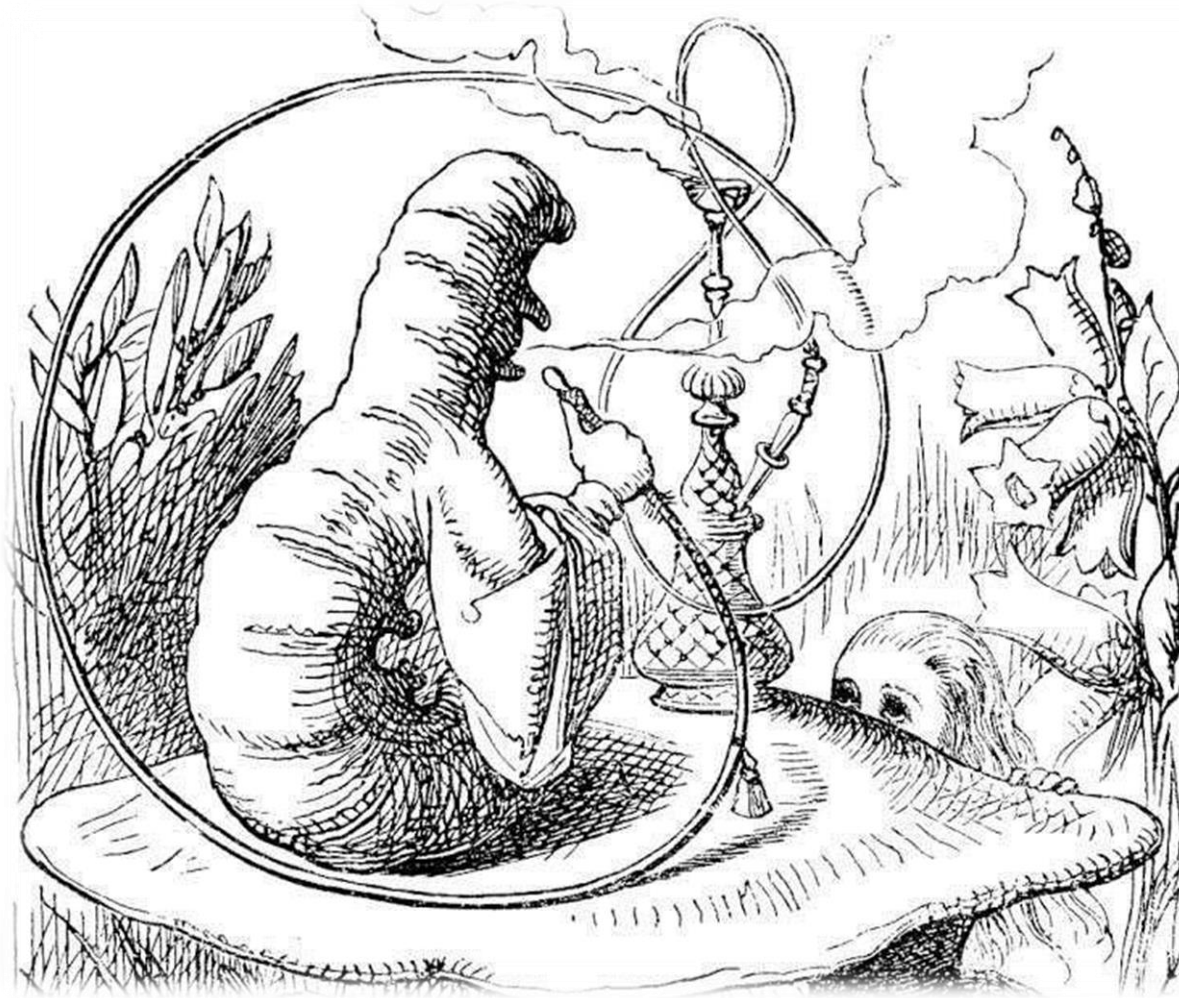
- Many of us rely on these devices daily.

- When we are at our most vulnerable, we will depend on these devices for life.

- Even at times when we aren't personally affected, people we care about may be.



Malicious Intent Is Not A Prerequisite To Patient Safety Issues



What We Are Doing

Medical Device Assessment

Discover patient safety issues

- Security-Focused Technical Assessment (not HIPAA)
- Research serves healthcare mission and values
- Equip defenders against accident and adversaries

Coordination & Notification

Alert affected parties

- Healthcare Providers
- Medical Device Manufacturers
- Government Agencies (FDA and ICS-CERT)

Public Awareness

Inoculate against future issues

- Security and Healthcare Conferences
- 1-on-1 with healthcare providers
- Educating FDA and Healthcare Providers



Phase 1 Research: Device Vulnerabilities

Phase 1 Research: Device Vulnerabilities

Weak default/hardcoded administrative credentials

- Treatment modification
- Cannot attribute action to individual

Known software vulnerabilities in existing and new devices

- Reliability and stability issues
- Increased deployment cost to preserve patient safety

Unencrypted data transmission and service authorization flaws

- Healthcare record privacy and integrity
- Treatment modification



Phase 2 Research: Internet Exposure

Shodan Search Initial Findings

Doing a search for anesthesia in Shodan and realized it was not an anesthesia workstation.

Located a public facing system with the Server Message Block (SMB) service open, and it was leaking intelligence about the healthcare organization's entire network including medical devices.



Initial Healthcare Organization Discovery



Very large US healthcare system consisting of over 12,000 employees and over 3,000 physicians. Including large cardiovascular and neuroscience institutions.

Exposed intelligence on over 68,000 systems and provided direct attack vector to the systems.

Exposed numerous connected third-party organizations and healthcare systems.

Did We Only Find One?

No. We found hundreds!!

Generic Search Examples:

shodan port:445 org:health*/clinic/hospital

health* - http://www.shodanhq.com/search?q=port:445+org:health*/clinic/hospital [.health](#) 148 hits

clinic - http://www.shodanhq.com/search?q=port:445+org:health*/clinic/hospital [clinic](#) 18 hits

hospital: http://www.shodanhq.com/search?q=port:445+org:health*/clinic/hospital [hospital](#) 119 hits

medical: http://www.shodanhq.com/search?q=port:445+org:health*/clinic/hospital [medical](#) 255 hits

Change the search term and many more come up. Potentially thousands if you include exposed third-party healthcare systems.

Summary Of Devices Inside Organization

Anesthesia Systems – 21

Cardiology Systems – 488

Infusion Systems – 133

MRI – 97

PACS Systems – 323

Nuclear Medicine Systems – 67

Pacemaker Systems - 31



Potential Attacks - Physical

▶ *We know what type of systems and medical devices are inside the organization.*

▶ *We know the healthcare organization and location.*

▶ *We know the floor and office number.*

▶ *We know if it has a lockout exemption.*



Potential Attacks - Phishing

▶ *We know what type of systems and medical devices are inside the organization.*

▶ *We know the healthcare organization and employee names.*

▶ *We know the hostname of all these devices.*

▶ *We can create a custom payload to only target medical devices and systems with known vulnerabilities.*

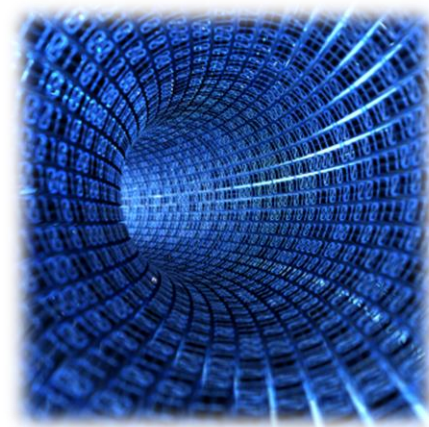


Potential Attacks - Pivot

▶ *We know the direct public Internet facing system is vulnerable to MS08-067 and is Windows XP.*

▶ *We know it is touching the backend networks because it is leaking all the systems it is connected to.*

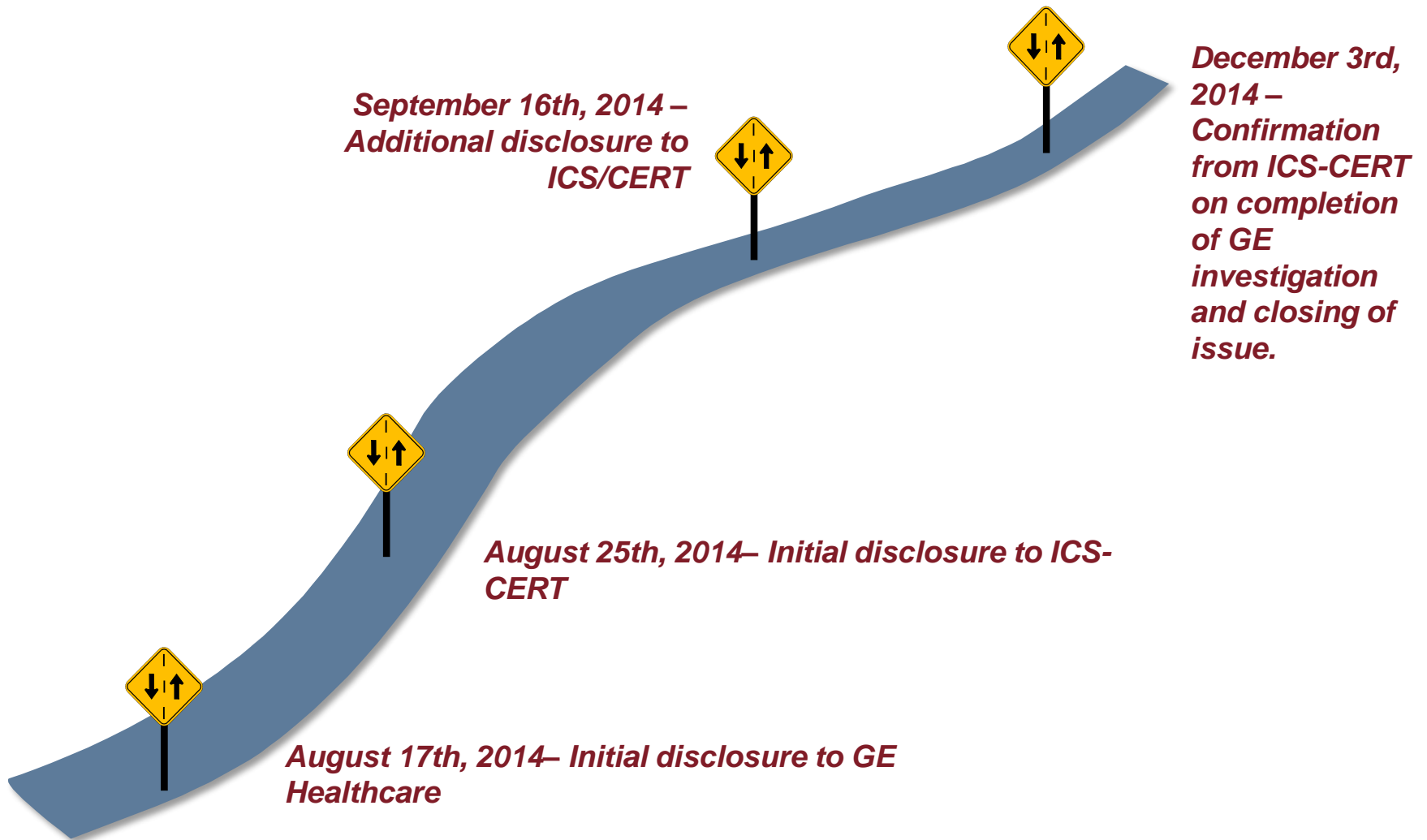
▶ *We can create a custom payload to pivot to only targeted medical devices and systems with known vulnerabilities.*





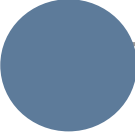
Phase 3 Research: Admin Access

Disclosure Timeline



NOTE: ALL INFORMATION DISCLOSED WAS PUBLICLY AVAILABLE ON GE HEALTHCARE'S WEBSITE.

Response



GE quickly responded to reports both from myself and ICS-CERT and outlined investigation plan for response.

After investigation GE responded that all credentials were default and not hard-coded.



CVE-2006-7253

GE Infinia II X4100 Workstation – Nuclear Imaging

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Infinia	II	X4100 Workstation Nuclear Imaging	Default User Account	UserID = "infinia" Password = "infinia"
GE	Infinia	II	X4100 Workstation Nuclear Imaging	FE or OLC Engineer Account	UserID = "acqservice" Password = "#bigguy1"
GE	Infinia	II	X4100 Workstation Nuclear Imaging	Administer Account-Window	UserID = "Administrator" Password = "dont4get2"
GE	Infinia	II	X4100 Workstation Nuclear Imaging	Emergency Account	UserID = "emergency" Password = "#bigguy1"
GE	Infinia	II	X4100 Workstation Nuclear Imaging	Administrator Account	UserID = "InfiniaAdmin" Password = "2Bfamous"

CVE-2013-7404

GE Discovery NM750b – Nuclear Imaging

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Discovery	NM 750b	Nuclear Imaging	Telnet- Root	UserID = "insite" Password = "2getin"
GE	Discovery	NM 750b	Nuclear Imaging	FTP- Admin	UserID = "insite" Password = "2getin"

CVE-2013-7404/CVE-2003-1603

CVE-2013-7407 GE Discovery NM750b – Nuclear Imaging

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Discovery	NM 750b	Nuclear Imaging	Telnet - Root	UserID = "insite" Password = "2getin"
GE	Discovery	NM 750b	Nuclear Imaging	FTP - Admin	UserID = "insite" Password = "2getin"

CVE-2003-1603 GE Discovery VH – Nuclear Imaging

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Discovery	VH	Nuclear Imaging	FTP - Remote Interfile Server	UserID = "ftpclient" Password = "interfile"
GE	Discovery	VH	Nuclear Imaging	FTP - Codonics Printer	UserID = "LOCAL" Password = "2"

CVE-2011-5374

CVE-2011-5374 GE Discovery NM670/NM630 - Nuclear Imaging/CT

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Discovery	NM670	Nuclear Imaging/CT	SU Account	UserID = "su" Password = "install"
GE	Discovery	NM670	Nuclear Imaging/CT	Service Account	UserID = "service" Password = "#bigguy1"
GE	Discovery	NM670	Nuclear Imaging/CT	Root Account	UserID = "root" Password = "install"
GE	Discovery	NM630	Nuclear Imaging	SU Account	UserID = "su" Password = "install"
GE	Discovery	NM630	Nuclear Imaging/CT	Service Account	UserID = "service" Password = "#bigguy1"
GE	Discovery	NM630	Nuclear Imaging/CT	Root Account	UserID = "root" Password = "install"

CVE-2009-5143

CVE-2009-5143 GE Discovery 530C - Nuclear Imaging

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Discovery	530C	Nuclear Imaging	Service Login	UserID = "acqservice" Password = "#bigguy1"
GE	Discovery	530C	Nuclear Imaging	Xeleris Service Login	UserID = "wsservice" Password = "#bigguy1"

CVE-2001-1594

CVE-2001-1594 GE eNTEGRA P&R - Nuclear Imaging

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	eNTEGRA P&R		Nuclear Imaging	Windows Admin	UserID = "entegra" Password = "entegra"
GE	eNTEGRA P&R		Nuclear Imaging	Polestar & Polestar-I Starlink 4	UserID = "super" Password = "passme"
GE	eNTEGRA P&R		Nuclear Imaging	Codonic Printer FTP Login	UserID = Your First Name Password = "300"
GE	eNTEGRA P&R		Nuclear Imaging	Codonic Printer FTP Login - User Preference File	UserID = "entegra" Password = "0"
GE	eNTEGRA P&R		Nuclear Imaging	eNTEGRA P&R User Account	UserID = "eNTEGRA" Password = "eNTEGRA"
GE	eNTEGRA P&R		Nuclear Imaging	Local Administrator Account	UserID = "Administrator" Password = "elgems"
GE	eNTEGRA P&R		Nuclear Imaging	WinVNC Login	Password = "insite"

CVE-2000-1253

CVE-2000-1253 GE FX Camera

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
<i>GE</i>	FX Camera		Camera	FX Camera Root Login	UserID = "root" Password = "vision"

CVE-2002-2445

CVE-2002-2445 GE Millennium MG/NC – Nuclear Imaging

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Millenium	MG and NC	Nuclear Imaging	Acquisition Root Login	UserID = "root" Password = "root.genie"
GE	Millenium	MG and NC	Nuclear Imaging	Acquisition Service Account	UserID = "service" Password = "service."
GE	Millenium	MG and NC	Nuclear Imaging	Acquisition Insite Login - Remote Support	UserID = "insite" Password = "insite.genieacq"
GE	Millenium	MG and NC	Nuclear Imaging	Acquisition Admin Login	UserID = "admin" Password = "admin.genie"
GE	Millenium	MG and NC	Nuclear Imaging	Acquisition Reboot Login	UserID = "reboot" Password = "reboot"
GE	Millenium	MG and NC	Nuclear Imaging	Acquisition Shutdown Login	UserID = "shutdown" Password = "shutdown"
GE	Millenium	MG and NC	Nuclear Imaging	Acquisition License Server Password	Password = "14geonly"

CVE-2002-2445 Continued

CVE-2002-2445 GE Millennium MyoSIGHT – Nuclear Imaging

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
<i>GE</i>	Millenium	MyoSIGHT	Nuclear Imaging	Acquisition Root Login	UserID = "root" Password = "root.genie"
<i>GE</i>	Millenium	MyoSIGHT	Nuclear Imaging	Acquisition Service Account	UserID = "service" Password = "service."
<i>GE</i>	Millenium	MyoSIGHT	Nuclear Imaging	Acquisition Insite Login - Remote Support	UserID = "insite" Password = "insite.genieacq"
<i>GE</i>	Millenium	MyoSIGHT	Nuclear Imaging	Acquisition Admin Login	UserID = "admin" Password = "admin.genie"
<i>GE</i>	Millenium	MyoSIGHT	Nuclear Imaging	Acquisition Reboot Login	UserID = "reboot" Password = "reboot"
<i>GE</i>	Millenium	MyoSIGHT	Nuclear Imaging	Acquisition Shutdown Login	UserID = "shutdown" Password = "shutdown"
<i>GE</i>	Millenium	MyoSIGHT	Nuclear Imaging	Acquisition Root Login	UserID = "root" Password = "root.genie"

CVE-2010-5306

CVE-2010-5306 GE Optima CT520/540/640/680 – CT Scanner

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Optima	CT680	CT Scanner	SU Login	UserID = "su" Password = "#bigguy"
GE	Optima	CT540	CT Scanner	SU Login	UserID = "su" Password = "#bigguy"
GE	Optima	CT640	CT Scanner	SU Login	UserID = "su" Password = "#bigguy"
GE	Optima	CT520	CT Scanner	SU Login	UserID = "su" Password = "#bigguy"

CVE-2010-5307

CVE-2010-5307 GE Optima MR360 - MRI

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Optima	MR360	MRI	Admin Login	UserID = "admin" Password = "adw2.0"
GE	Optima	MR360	MRI	System Startup Login	UserID = "sdc" Password = "adw2.0"

CVE-2014-7233/CVE-2014-7234

CVE-2014-7233 GE Precision THUNIS-800+ – X-Ray

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Precision	THUNIS-800+	X-Ray	Factory Default Service Password	Password = "1973"
GE	Precision	THUNIS-800+	X-Ray	TH8740 Software/Firmware Package Password	Password = "TH8740"
GE	Precision	THUNIS-800+	X-Ray	DSA Software Package Password	Password = "hrml"

CVE-2014-7234 GE Precision THUNIS-800+ – X-Ray

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Precision	THUNIS-800+	X-Ray	Shutter Configuration Password	No Username Or Password Required To Login

CVE-2012-6660/CVE-2010-5310

CVE-2012-6660 GE Precision MPI – X-Ray

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Precision	MPI	X-Ray	Windows XP Service Login (Press & Hold Left Shift Key After Setup Dialog)	UserID = "serviceapp" Password = "orion"
GE	Precision	MPI	X-Ray	Clinical Operator Login	UserID = "operator" Password = "orion"
GE	Precision	MPI	X-Ray	Administrator Login	UserID = "administrator" Password = "PlatinumOne"

CVE-2012-6660 GE Precision MPI – X-Ray

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Revolution	XQ/i	X-Ray	System Startup Login - Acquisition Workstation	UserID = "sdc" Password = "adw3.1"
GE	Revolution	XR/d	X-Ray	System Startup Login - Acquisition Workstation	UserID = "sdc" Password = "adw3.1"

CVE-2013-7405

CVE-2013-7405 GE Centricity DMS 4.0/4.1/4.2 – Cardiology Application

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Centricity DMS	4.2.x	Cardiology Application	Administrator Login	UserID = "Administrator" Password = "Never!Mind"
GE	Centricity DMS	4.2.x	Cardiology Application	Muse Admin Login	UserID = "Museadmin" Password = "Muse!Admin"
GE	Centricity DMS	4.1.x	Cardiology Application	Muse Admin Login	UserID = "Museadmin" Password = "Muse!Admin"
GE	Centricity DMS	4.0.x	Cardiology Application	Muse Admin Login	UserID = "Museadmin" Password = "Muse!Admin"

CVE-2004-2777

CVE-2004-2777 GE Centricity Image Vault – Cardiology

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Centricity Image Vault		Cardiology	Administrator Login	UserID = "administrator" Password = "gemnet"
GE	Centricity Image Vault		Cardiology	Webadmin Administrator Login	UserID = "administrator" Password = "webadmin"
GE	Centricity Image Vault		Cardiology	SQL SA Ultrasound Database Login	UserID = "gemsservice" Password = No Password Required
GE	Centricity Image Vault		Cardiology	GEMNet License Server Login	UserID = "gemnet2002" Password = "gemnet2002"

CVE-2014-9736

CVE-2014-9736 GE Centricity Archive Audit Trail

<i>Manufacturer</i>	<i>Model</i>	<i>Type of Account</i>	<i>Login info</i>
<i>GE</i>	Centricity Clinical Archive Audit Trail Repository	SSL Key Manager Password	initnit
<i>GE</i>	Centricity Clinical Archive Audit Trail Repository	Server Keystore Password	initnit
<i>GE</i>	Centricity Clinical Archive Audit Trail Repository	Server Truststore Password	keystore_password
<i>GE</i>	Centricity Clinical Archive Audit Trail Repository	Database Primary Storage Login	UserID = "atna" Password = "atna"
<i>GE</i>	Centricity Clinical Archive Audit Trail Repository	Database Archive Storage Login	UserID = "atna" Password = "atna"

CVE-2011-5322

CVE-2011-5322 GE Centricity Analytics Server

<i>Manufacturer</i>	<i>Model</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Centricity Analytics Server	SQL SA Login	UserID = "sa" Password = "V0yag3r"
GE	Centricity Analytics Server	Analytics & Dundas Account Login	UserID = "analyst" Password = "G3car3s"
GE	Centricity Analytics Server	Analytics CCG Login	UserID = "ccg" Password = "G3car3s"
GE	Centricity Analytics Server	Analytics Viewer Login	UserID = "viewer" Password = "V0yag3r"
GE	Centricity Analytics Server	Analytics Real-time Dashboard Admin Login	UserID = "admin" Password = "V0yag3r"
GE	Centricity Analytics Server	Analytics CCG Webmin Service Tool Login	UserID = "geservice" Password = "geservice"

CVE-2011-5323

CVE-2011-5323 GE Centricity PACS

<i>Manufacturer</i>	<i>Model</i>	<i>Type of Account</i>	<i>Login info</i>
<i>GE</i>	Centricity PACS-IW 3.7.3.8	SQL SA Login	UserID = "sa" Password = "A11endale"
<i>GE</i>	Centricity PACS-IW 3.7.3.7	SQL SA Login	UserID = "sa" Password = "A11endale"

CVE-2011-5324

CVE-2011-5324 GE Centricity PACS

<i>Manufacturer</i>	<i>Model</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Centricity PACS-IW 3.7.3.8	TeraRecon Server Shared Login	UserID = "shared" Password = "shared" Group = "shared"
GE	Centricity PACS-IW 3.7.3.8	TeraRecon Server Scan Login	UserID = "scan" Password = "scan" Group = N/A
GE	Centricity PACS-IW 3.7.3.7	TeraRecon Server Shared Login	UserID = "shared" Password = "shared" Group = "shared"
GE	Centricity PACS-IW 3.7.3.7	TeraRecon Server Scan Login	UserID = "scan" Password = "scan" Group = N/A

CVE-2012-6693

CVE-2012-6693 GE Centricity PACS Server

<i>Manufacturer</i>	<i>Model</i>	<i>Type of Account</i>	<i>Login info</i>
<i>GE</i>	Centricity PACS 4.0 Server	NAS Read Only Login	UserID = "nasro" Password = "nasro"
<i>GE</i>	Centricity PACS 4.0 Server	NAS Read/Write Login	UserID = "nasrw" Password = "nasrw"

CVE-2012-6694

CVE-2012-6694 GE Centricity PACS

<i>Manufacturer</i>	<i>Model</i>	<i>Type of Account</i>	<i>Login info</i>
<i>GE</i>	Centricity PACS 4.0.1 Workstation	TimbuktuPro Remote Control Software Service Login	UserID = "geservice" Password = "2charGE"
<i>GE</i>	Centricity PACS 4.0.1 Workstation	GE Service Account Login	UserID = "geservice" Password = "2charGE"
<i>GE</i>	Centricity PACS 4.0.Workstation	TimbuktuPro Remote Control Software Service Login	UserID = "geservice" Password = "2charGE"
<i>GE</i>	Centricity PACS 4.0.Workstation	GE Service Account Login	UserID = "geservice" Password = "2charGE"
<i>GE</i>	Centricity PACS 4.0 Server	GE Service Account Login	UserID = "geservice" Password = "2charGE"

CVE-2012-6695

CVE-2012-6694 GE Centricity PACS

<i>Manufacturer</i>	<i>Model</i>	<i>Type of Account</i>	<i>Login info</i>
<i>GE</i>	Centricity PACS 4.0.1 Workstation	DDP Admin Login	UserID = "ddpadmin" Password = "ddpadmin"
<i>GE</i>	Centricity PACS 4.0.Workstation	DDP Admin Login	UserID = "ddpadmin" Password = "ddpadmin"

CVE-2013-7442

CVE-2013-7442 GE Centricity PACS

<i>Manufacturer</i>	<i>Model</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Centricity PACS 4.0.1 Workstation	Administrator Login	UserID = "Administrator" Password = "CANa11"
GE	Centricity PACS 4.0.1 Workstation	IIS Login	UserID = "iis" Password = "iis"
GE	Centricity PACS 4.0.Workstation	Administrator Login	UserID = "Administrator" Password = "CANa11"
GE	Centricity PACS 4.0.Workstation	IIS Login	UserID = "iis" Password = "iis"

Additional Disclosures – CVE Pending

CVE-2003-???? GE Gamma Camera

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
<i>GE</i>	DST/DST-XL/DST-Xli/DSXi/DSTi/Dsi	Software Version 8.0.3	Gamma Camera	Camera Configuration	Password = "sopha"
<i>GE</i>	DST/DST-XL/DST-Xli/DSXi/DSTi/Dsi	Software Version 8.0.1	Gamma Camera	Camera Configuration	Password = "sopha"
<i>GE</i>	DST/DST-XL/DST-Xli/DSXi/DSTi/Dsi	Software Version 7.9.7	Gamma Camera	Camera Configuration	Password = "sopha"
<i>GE</i>	DST/DST-XL/DST-Xli/DSXi/DSTi/Dsi	Software Version 7.7.19	Gamma Camera	Camera Configuration	Password = "sopha"

Additional Disclosures – CVE Pending

CVE-????-????1 GE HiSpeed - CT Scanner

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	HiSpeed Adv	CTI	CT Scanner	SU Login	UserID = "su" Password = "#bigguy")"
GE	HiSpeed Adv	CTI	CT Scanner	PROM Reset Password Command - No Password Required	Command = "resetpw"
GE	HiSpeed	NP	CT Scanner	SU Login	UserID = "su" Password = "#bigguy"
GE	HiSpeed Adv	Z	CT Scanner	SU Login	UserID = "su" Password = "genesis"
GE	HiSpeed Adv	Z	CT Scanner	Root Login	UserID = "root" Password = "#bigguy"
GE	HiSpeed Adv	Z	CT Scanner	Genesis Login	UserID = "genesis" Password = "4\$app"
GE	HiSpeed Adv	Z	CT Scanner	Insite Login	UserID = "insite" Password = "2getin"
GE	HiSpeed Adv	Z	CT Scanner	Service Login	UserID = "service" Password = "4rhelp"
GE	HiSpeed Adv	Z	CT Scanner	Genesis Sun Computer Root Login	UserID = "root" Password = "Genesis"

Additional Disclosures – CVE Pending

CVE-????-????1 GE HiSpeed - CT Scanner

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	HiSpeed Adv	RP	CT Scanner	SU Login	UserID = "su" Password = "#bigguy"
GE	HiSpeed Adv	RP	CT Scanner	Root Login	UserID = "root" Password = "#bigguy"
GE	HiSpeed Adv	RP	CT Scanner	Insite Login	UserID = "insite" Password = "2getin"
GE	HiSpeed Adv	RP	CT Scanner	Genesis Login	UserID = "genesis" Password = "4\$app"
GE	HiSpeed Adv	RP	CT Scanner	Service Login	UserID = "service" Password = "4rhel"
GE	HiSpeed Adv	RP	CT Scanner	Genesis Sun Computer Root Login	UserID = "root" Password = "Genesis"
GE	HiSpeed Dual	ProSpeed FII	CT Scanner	SU Login	UserID = "su" Password = "#bigguy"
GE	HiSpeed	Qx/i	CT Scanner	SU Login	UserID = "su" Password = "#bigguy"

Additional Disclosures – CVE Pending

CVE-????-????

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
<i>GE</i>	Optima	MR360	MRI	Emergency Login	No Username Or Password Required To Login
<i>GE</i>	CADStream Server		MRI	Admin Login (In Addition Password Manager Will Remember Login And Never Require Future Login)	UserID = "admin" Password = "confirma"

Additional Disclosures – CVE Pending

CVE-????-???? GE Precision MPi – X-Ray

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Precision	MPi	X-Ray	Service Tech 1 & Service Tech 2 Login (Created Using CreateServiceUsers.bat Script)	UserID = "servicetech1" & "servicetech2" Password = "servicetech"
GE	Precision	MPi	X-Ray	User Accounts Tech 1 through Tech 20 Login (Created Using CreateUsers01-20.bat Script)	UserID = "Tech1" through "Tech20" Password = "xraytech"
GE	Precision	MPi	X-Ray	User Accounts Tech 21 through Tech 40 Login (Created Using CreateUsers21-40.bat Script)	UserID = "Tech21" through "Tech40" Password = "xraytech"
GE	Precision	MPi	X-Ray	User Accounts Tech 41 through Tech 60 Login (Created Using CreateUsers41-60.bat Script)	UserID = "Tech41" through "Tech60" Password = "xraytech"
GE	Precision	MPi	X-Ray	User Accounts Tech 61 through Tech 80 Login (Created Using CreateUsers61-80.bat Script)	UserID = "Tech61" through "Tech80" Password = "xraytech"
GE	Precision	MPi	X-Ray	User Accounts Tech 81 through Tech 100 Login (Created Using CreateUsers81-100.bat Script)	UserID = "Tech81" through "Tech100" Password = "xraytech"

[illegible]

So If They Are Indeed Default Are There Still Issues

- Documentation instructs in some cases to not change credentials and not allow password reset.
- Documentation instructs in some cases to not change password or your account will not be able to be supported.
- Documentation not updated with how to change default credentials and secure configuration guides are lacking.
- Support personal often rely on implementation documentation so these logins are heavily utilized in the healthcare industry.

Examples

3. When the *User Properties* screen appears, verify/change the following parameters and click **OK**.

- ◆ *User Must Change Password at Next Login*: Unchecked
- ◆ *User Cannot Change Password*: Checked
- ◆ *Password Never Expires*: Checked
- ◆ *Account Disabled*: Uncheck

Emergency Login

Click **Emergency Login** to launch the Emergency Login screen which does not require a ID or password that is filed on your Enterprise system.

3.3.2 Changing Passwords

You can change any of the account passwords with the following procedure.

Important

Do not change the InSite password. Remote access will be disabled for InSite support if the password is changed.

Examples

Table 3-8: Acquisition Passwords

Account User Name	Default Password
root	root.genie
service	service.
insite	insite.genieacq (Do not change this password!)
admin	admin.genie
reboot	reboot
shutdown	shutdown

Examples

Name	Password
MuseAdmin	Muse!Admin

NOTE: Tech Support will logon to the system with pcAnywhere using this user name and password.



Examples

Ask the remote station operator for your assigned username and **password**.

This resets the user's confirm password to **password**.

NOTE: To perform the following steps, you must generate X-ray radiation. Follow proper safety precautions with the X-ray system.

1. Turn on the digital system and login as service:
(user: **serviceapp** password: **orion**)
2. When the service application starts, select the **Calib** function on the *Main Menu*.
3. Select **System Manual Tab**.
4. Select **Overlay Tab**.
5. You should now see a white circle in the image display (you may want to minimize the calibration window). Activate fluoro radiation; center the II output phosphor within the outline circle by moving the camera/lens assembly position on the image intensifier (II).

Examples

WARNING



Adhere strictly to the procedures in this manual.

Some repair/replacement procedures require the removal of protective covers, exposing parts which may be heated to a high temperature, or potential pinch points.

To prevent burns or other injuries, read the safety/warning labels.



The editors and producers of this GE documentation site claim no responsibility for the accuracy, content, or availability of information contained on this site, or accessed or linked to through use of this site.



Is AppSec a Problem?

Is AppSec A Problem?

You Decide

RawParamsHeadersHex

POST /formPrivacyProc HTTP/1.1
Host:
Connection: keep-alive
Content-Length: 368
Cache-Control: max-age=0
Authorization: Basic YWRtaW46SDBzcDFyYQ==
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin:
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: /formWlanProc
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8

WlanSecurityType=enterprise&WpaEncryption=CCMP&WlanAuthType=OPEN&WepKeyLen=WEP40&WlanKey0=&WlanKey1=&WlanKey2=&WlanKey3=&WepDefKeyId=0&WpaSharedKey=&WpaEapType=peap&TtlsProtocol=eap-msc
happv2&PeapInnerProtocol=eap-mschapv2&WpaIdentity=&WpaPswd=&WpaPswdConfirm=&WpaAnonIdentity=&NextPage=next&AppTimeStamp=487-1104&WpaFastPacFile=

WlanSecurityType=enterprise&WpaEncryption=CCMP&WlanAuthType=OPEN&WepKeyLen=WEP40&WlanKey0=&WlanKey1=
happv2&PeapInnerProtocol=eap-mschapv2&WpaIdentity=&WpaPswd=&WpaPswdConfirm=

=&WlanKey2=&WlanKey3=&WepDefKeyId=0&WpaSharedKey=&WpaEapType=peap&TtlsProtocol=eap-msc
&WpaAnonIdentity=&NextPage=next&AppTimeStamp=487-1104&WpaFastPacFile=



Diagnosis

Technical Properties



Exposed, vulnerable systems

- All software has flaws.
- Connectivity increases potential interactions.
- A software-driven, connected medical device is a **vulnerable, exposed** one.



Lack of patient safety alignment in medical device cyber security practices

Problem Awareness



1

***Medical devices** are **increasingly accessible** due to the nature of healthcare*

2

*HIPAA focuses on patient privacy, not **patient safety**.*

3

***FDA does not** validate **cyber safety** controls.*

4

***Malicious intent** is **not** a prerequisite for adverse patient outcomes.*



Treatment Plans

Treatment Plans

- Scan your biomedical device environment for default credentials.
- Report identified issues to manufacturer for remediation in your environment.



Treatment Plans

*It falls to all of us. Patient safety is not a **spectator sport**.*



- **Stakeholders** must **understand** prerequisites
- **Multi-stakeholder** teams and conversations
- Engage with **willing allies** where domains of expertise overlap
- Incorporate **safety** into **existing processes**

Continue As-Is

Summary of Current State

- FDA receives “several hundred thousand” reports of patient safety issues per year related to medical devices
- Cyber safety investigations hampered by evidence capture capabilities.
- New devices are coming to market with long-known defects.
- Existing devices aren’t consistently maintained and updated.

Projected Future

- The nature of healthcare is driving towards greater connectivity (and therefore exposure) of devices.
- Adversaries change the risk equation unpredictably
- Increase in incidental contact

A Better Way

Summary of Recommended Treatment

- Patient safety as the overriding objective
- Avoid failed practices and iteratively evolve better ones
- Engage internal and external stakeholders
- Safety into existing practices and governance

Projected Outcomes

- “Reliable medical devices to market without undue delay or cost.”
- Collaboration among willing allies on common terms
- Medical devices resilient against accidents and adversaries

How To Get Involved

☐ Acquiring Medical Devices – eBay or MedWow

☐ Get Involved In Industry Working Groups

☐ Speak On Topic At Industry Conferences

☐ I Am The Cavalry

<https://iamthecavalry.org>



I Am The Cavalry

Q & A

