Zingbox

# Discovery of Cyberattack Trends Targeting Connected Medical Device

## WHITE PAPER

Detailed analysis of hackers leveraging device error messages

## Executive Summary

A Hacker can learn important system and device details from the information available in error messages. By analyzing this information, the hacker can tailor the attack to exploit vulnerabilities associated with the OS and applications running on the device, greatly increasing the chance of successful attack. Zingbox security researchers uncovered this latest trend of accelerating cyberattacks and have notified various device manufacturers. This report outlines the details of the latest trend along with information on the device manufacturers and their schedule of patch releases. One remedy being implemented by manufacturers is to provide error details via debugging tools and other secure means rather than in error messages.

## Background

The first phase of attackers trying to hack a device is called “information/Intelligence gathering” . This phase helps attackers understand the inner workings of the device; the type of web server, framework, and software versions used; the manufacturer that developed it; the database engine in the back end; and the protocols used. Once the attacker collects this information, he can launch a more focused attack, and a rule of thumb is and always will be: The more data collected, the higher chance of success.

One of the commons ways for an attacker to collect this data is by analyzing error messages originating from the application in the device such as stack traces, SQL errors, and file system errors.

There are two main ways to gather this information:

1. **Passive** - The attacker waits for an error to be triggered without attacking the system. In this scenario, the application sends errors during authentication failures, database connectivity issues, file systems full, timeouts, and so on. With this approach, an attacker with access to the LAN just needs to sniff the network and wait for these errors to flow by.
2. **Active** - The attacker sends malformed or unexpected requests to the web server and waits to receive error messages normally caused due to unhandled exceptions.

Let’s imagine an application that is sending an error message with the following information:

- Tomcat version
- Windows file location. E.g. c:\winnt\file
- Oracle database version
- WordPress CMS
- Database username

When an attacker receives the error message, he can take the following actions:

- Check if there are vulnerabilities for the different components identified based on their version.
- Brute force the authentication mechanism now that the username is known as well as the database engine.

- Focus on Windows-only attacks.

As you can see, the more data you obtain, the higher chances of the attack being successful.

OWASP names this issue as “Improper Error Handling”.

https://www.owasp.org/index.php/Improper_Error_Handling

Remediation examples:

https://www.owasp.org/index.php/Error_Handling

MITRE names this issue as “Information Exposure Through an Error Message”.

https://cwe.mitre.org/data/definitions/209.html

During this research, Zingbox uncovered multiple IoT devices leaking technical and sometimes sensitive information. The issues were reported to vendors via ICS-CERT, but unfortunately only one manufacturer has issued a patch to-date. This report shares our findings with the larger community in the hopes that hospitals and other provider organizations relying on these devices can take necessary steps to secure their devices.

## Overview of Findings

Below is a list of devices found leaking sensitive or technical information due to improper error handling issues.

| Manufacturer | Device Description | Vendor notification via ICS-CERT | Plan to release patch |
|---|---|---|---|
| Fujifilm | Synapse PACS (medical imaging) | May 3, 2018 | Not planning to release a patch |
| Johnson Controls | Metasys & BCPro (smart building) | May 14, 2018 | Patch released CVE-2018-10624 |
| Siemens | Syngo PACS (medical imaging) | May 16, 2018 | Not planning to release a patch |
| Change Healthcare/peerVue | peerVue PACS (medical imaging) | June 29, 2018 | Vendor planning to issue a patch |
| CareStream | Vue RIS (radiology system) | July 9, 2018 | Vendor planning to issue a patch |
| CBORD | Healthcare management system | July 30, 2018 | Waiting for vendor acknowledgement |
| Nuance | Radiology RAS application | August 28, 2018 | Waiting for vendor acknowledgement |

Note: The above order is based on the time vendors were notified.

# Detailed Findings

Note: All the sensitive methods, class names, parameters, database details, server names, and paths have been masked out of the following error messages.

## Fujifilm – Synapse PACS

### Vendor information

http://www.fujifilmusa.com/products/medical/medical-informatics/radiology/communications/

### Type of information disclosed via error message

- Data Base running in the server
- Software Stack Trace
- Database usernames

### Leaked information via HTTP 500 Error

```
48 54 54 50 2F 31 2E 31 20 35 30 30 20 49 6E 74  HTTP/1.1 500 Int
 65 72 6E 61 6C 20 53 65 72 76 65 72 20 45 72 72  ernal Server Err
.
.
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 72  -1..Server: XXXX
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 73  XXXXXXXXXXXXX..s
 79 6E 61 70 73 65 2D 74 69 6D 65 64 65 74 61 69  ynapse-timedetai
 6C 3A 20 74 6F 74 61 6C 3D 31 30 33 39 31 20 53  l: total=10391 S
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6C  ettingsXXXXHandl
 65 72 20 47 45 54 20 63 6F 6D 2E 66 75 6A 69 6D  er GET com.fujim
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5F  ed.Login.XXXXXX_
 42 30 36 39 32 30 45 39 33 45 30 31 34 39 44 44  B06920E93E0149DD
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44  97E67F0XXXXXDF9D
 2E 78 6D 6C 20 74 69 6D 65 3D 30 2C 20 3E 43 61  .xml time=0, >Ca
 63 68 69 6E 67 48 61 6E 64 6C 65 72 20 63 61 63  chingHandler cac
 68 65 20 74 69 6D 65 3D 30 2C 20 3E 3E 44 42 2E  he time=0, >>DB.
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6D  GetXxx com.fujim
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 35 5F  ed.Login.XXXXXX_
 42 30 36 39 32 30 45 39 33 45 30 31 34 39 44 44  B06920E93E0149DD
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44  97E67F0XXXXXDF9D
 2E 78 6D 6C 20 49 66 4E 6F 6E 65 4D 61 74 63 68  .xml IfNoneMatch
 3D 31 37 39 20 66 69 6C 74 65 72 42 79 4D 61 63  =179 filterByMac
 68 69 6E 65 3D 63 6F 6D 2E 66 75 6A 69 6D 65 64  hine=com.fujimed
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 49  .Machine.XXXXX_I
 53 31 38 30 39 32 32 33 5F 51 47 43 41 4A 5A 36  S1809223_QGCAJZ6
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44  XXXXXXFBJ4AOH2KD
 58 33 34 2E 78 6D 6C 20 74 69 6D 65 3D 31 30 33  X34.xml time=103
 39 31 2C 20 3E 3E 3E 44 42 2E 4F 70 65 6E 20 44  91, >>>DB.Open D
 61 74 61 62 61 73 65 20 43 6F 6E 6E 65 63 74 69  atabase Connecti
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70  on time=0..XXXXX
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30  XXXXVersion: 4.0
```

```
2E 33 30 33 31 39 0D 0A 50 65 72 73 69 73 74 65  .30319..Persiste
6E 74 2D 41 75 74 68 3A 20 74 72 75 65 0D 0A 58  nt-Auth: true..X
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50  -Powered-By: XXX
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2C  .XXX..Date: Wed,
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3A   28 XXX 201X 05:
33 36 3A 30 30 20 47 4D 54 0D 0A 43 6F 6E 74 65  36:00 GMT..Conte
6E 74 2D 4C 65 6E 67 74 68 3A 20 38 37 31 0D 0A  nt-Length: 871..
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 63  ..XXXXXXXXX.XAcc
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6C  ess.Client.Xxxxx
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30  xException XX-XX
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6C  XXX: xxxxxxxxxxx
65 20 6F 6E 20 63 6F 6D 6D 75 6E 69 63 61 74 69  e on communicati
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 65  on chxxxxx.Proce
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 65  ss ID: 3XX748.Se
73 73 69 6F 6E 20 49 44 3A 20 31 38 33 38 20 53  ssion ID: 1838 S
65 72 69 61 6C 20 6E 75 6D 62 65 72 3A 20 34 37  erial number: 47
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2E  79    at XXXXXX.
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6E  XxxxAccess.Clien
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6F  t.XXXXXXException
6E 2E 48 61 6E 64 6C 65 45 72 72 6F 72 48 65 6C  n.HandleErrorHel
70 65 72 28 49 6E 74 33 32 20 65 72 72 43 6F 64  per(Int32 errCod
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 74  e, Connect xxxxx
69 6F 6E 20 63 6F 6E 6E 2C 20 49 6E 74 50 74 72  ion conn, IntPtr
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53   opsCtx, xxxxxoS
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 71  xxValCtx* xxpoSq
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20  lVxxxxtx, Object
73 72 63 2C 20 53 74 72 69 6E 67 20 70 72 6F 63  src, String proc
```

## Johnson Controls - Metasys & BCPro Smart Buildings

### Vendor information

https://www.johnsoncontrols.com/buildings/building-management/building-automation-systems-bas

### Patch released

https://ics-cert.us-cert.gov/advisories/ICSA-18-212-02

### Type of information disclosed via error message

- Software Stack Trace
- Source code line numbers where failure occurs
- Server File System Path

### Leaked information via HTTP 500 Error

```
HTTP/1.1 500 Internal Server Error

Cache-Control: private
Content-Type: text/xml; charset=utf-8
Server: <Web Server Type and Version>
Date: Wed, 02 XX 2018 02:19:47 GMT
Content-Length: 118
```

```
<?xml version="1.0" encoding="utf-8"?><soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><soap:Body><soap:Fault><faultcode>soap:Server</fault
code><faultstring>System.Web.Services.Protocols.SoapException: XXXXXXXXX ---&gt;
System.ApplicationException: XXXXXXX
   at JohnsonControls.MetasysIII.XXXXX.XXXXX(String xxxxx, String xxxxx, Int32 xxxxx) in
x:\xxxx\xxxx.xxx\xxxxxx\xxxxxxxxxxxx:line 1042
   at JohnsonControls.MetasysIII.xxxx.xxxx.xxxx(XmlNode xxxData) in
x:\xxxx\xxxx.xxx\xxxxxx\xxxxxxxxxxxx:line:line 288
   --- End of inner exception stack trace ---
```

## Siemens - Syngo PACS

### Vendor information

https://www.healthcare.siemens.com/medical-imaging-it

### Type of information disclosed via error message

- Software Stack Trace
- Source code methods and parameters

### Leaked information via HTTP 500 Error

```
HTTP/1.1 500 Internal Server Error

Cache-Control: private
Content-Type: text/xml; charset=utf-8
Server: <Web Server Type and Version>
Date: Mon, 14 XX 2018 15:06:08 GMT
Content-Length: 130
```

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><s:Fault><faultcode
xmlns:a="http://schemas.microsoft.com/net/2005/12/windowscommunicationfoundation/dispatcher">a:InternalServiceFa
ult</faultcode><faultstring xml:lang="en-US">Invalid user name or
password.</faultstring><detail><ExceptionDetail
xmlns="http://schemas.datacontract.org/2004/07/System.ServiceModel" xmlns:i="http://www.w3
.org/2001/XMLSchema-instance"><HelpLink i:nil="true"/><InnerException i:nil="true"/><Message>Invalid user name
or password.</Message><StackTrace>   at XXX.XXX.XXXXX.XXXXUser(Credentials cred, String pass,
DatabaseType DatabaseType)&#xD;
   at XXX.XXX.XXXXX.XXXXHelper(String Name, String password, String AccounXX, String requesXX, String
XXXXInfo, DatabaseType DatabaseType, String[] flags)&#xD;
<- cut for brevity -->
StackTrace><Type>System.Configuration.Provider.ProviderException</Type></ExceptionDetail></detail
></s:Fault></s:Body></s:Envelope>
```

## Change Healthcare - peerVue PACS

### Vendor information

https://www.changehealthcare.com/solutions

### Type of information disclosed via error message

- Stack Trace

- Class Names and arguments

### Leaked information via HTTP 500 Error

```
HTTP/1.1 500 Internal Server Error

Cache-Control: private
Content-Type: text/xml; charset=utf-8
Server: <Web Server Type and Version>
Content-Length: 99
<?xml version="1.0" encoding="utf-8"?><soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><soap:Body><soap:Fault><faultcode>soap:Server</fault
code><faultstring>System.Web.Services.Protocols.SoapException: Server was unable to process
request. ---&gt; System.Runtime.XXXX.XXXXX: OpenXXX,XXXPath,XXXMode
   at System.RuntimeType.FXXXXXMember(String memberName, BindingFlags flags, Object target,
Int32[] aWrapperTypes, MessageData&amp; msgData)
   at XXXXInstaller.Installer.OpeXXX (String XXXXPath, Object XXXMode)
   at XXX.PeerVue.peerVueXXXXXX.GetPeerVueVersion(String physicalPath)
   at PeerVueService.XXXPeerVueSetupsVersion(String path)
   --- End of inner exception stack trace ---</faultstring><detail
/></soap:Fault></soap:Body></soap:Envelope>
```

## CareStream - Vue RIS  Radiology System

### Vendor information

https://www.carestream.com/en/us/medical/products/vue-healthit/radiology/carestream-vue-ris

### Type of information disclosed via error message

- Data Base running in the server
- Software Stack Trace
- Source code line numbers where failure occurs
- Server File System Path

### Leaked Information via HTTP 500 Error

```
HTTP/1.1 500 Internal Server Error

Cache-Control: private
Content-Length: 369
Content-Type: text/html; charset=utf-8
Server: <Web Server Type and Version>
Date: Tue, 05 XXX 2018 10:21:35 GMT

<html>
    <head>
        <title>DATABASE ERROR CODE<br></title>
    </head>
    <body bgcolor="white">
            <span><H1>Server Error in '/XXXXX_PROD/XXXXX-WS' Application.<hr width=100% size=1
color=silver></H1>
            <h2> <i> DATABASE ERROR CODE <br></i> </h2></span>
```

```
            <font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">
            <b> Description: </b>An unhandled exception occurred during the execution of the
current web request. Please review the stack trace for more information about the error and where
it originated in the code.
            <br><br>
            <b> Exception Details: </b>STACK TRACE ERROR<br><br><br>
            <b>Source Error:</b> <br><br>
←cut for brevity-->
                        <code><pre>
                                        FULL STACK TRACE ERROR
MonitorConnection) in Server File System Path
Source code line numbers:31
Source code line numbers:145
Source code line numbers:220
Source code line numbers:111
Source code line numbers () +127
Source code line numbers) +76
←cut for brevity-->
```

## CBORD - Healthcare Management System

### Vendor information

https://www.cbord.com/industries/healthcare/

### Type of information disclosed via error message

- Stack Trace
- Class Names and arguments
- Source code line numbers where failure occurs

### Leaked information via HTTP 500 Error

```
HTTP/1.1 500 Internal Server Error

Cache-Control: private
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
X-Robots-Tag: noindex,nofollow,notranslate
Date: Mon, 16 XX 2018 20:36:20 GMT
Content-Length: 1387
<!DOCTYPE html>
<html>
    <head>
        <title>DataXXXager: Exception during call of method 'XXXXJSON' in class 'ActXXXXXX:
Trusted authentication failed because 'XXXXabled'; cannot continue</title>
        <cut for brevity…>
<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">
            <b> Description: </b>An unhandled exception occurred during the execution of the
current web request. Please review the stack trace for more information about the error and where
it originated in the code.
            <br><br>
```

```
            <b> Exception Details: </b>CBORD.XXX.Framework.XXX.XXXException: DataXXXager:
Exception during call of method 'XXXXJSON' in class XXXXXXXXX: Trusted authentication failed
because 'XXXXXabled'; cannot continue<br><br>
            <b>Source Error:</b> <br><br>
            <table width=100% bgcolor="#ffffcc">
               <tr>
  <table width=100% bgcolor="#ffffcc">
               <tr>
                  <td>
                      <code><pre>
Source code line numbers Object[] parms) +1366
Source code line numbers Boolean something) +240
Source code line numbers Boolean ReloadLists) +305
Source code line numbers Object[] ) +503
Source code line numbers parameters) +229
Source code line numbers b__3d() +72
<!--
[CBORDException]: … cannot continue
   at CBORD.XX.XXXXXX.XXXXXX.XXXX(IUXXntext ctx, String asxxxxbly, String method, Object[] parms)
   at CBORD.XX.XXXXXX.XXXX.XXXXJson(IXXXontext ctx, String tracXXXXId, String CheckXXXtId,
Boolean something)
```

## NUANCE – Radiology RAS Application

### Vendor information

https://www.nuance.com/healthcare/medical-imaging.html

### Type of information disclosed via error message

- Stack Trace
- Class Names and arguments

## Leaked information via HTTP 500 Error

```
HTTP/1.1 500 Internal Server Error
Content-Length: 1651
Content-Type: application/soap+xml; charset=utf-8
Server: XXXXXXXX
X-Powered-By: ASP.NET
Date: XX, xx Aug 2018 12:32:22 GMT

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <a:Action s:Understand="1">http://www.w3.org/2005/08/addressing/soap/fault
    </a:Action>
    <a:RelatesTo>urn:uuid:1f4aea5f-4abe-4845-a498-36e9c571ff4e</a:RelatesTo>
  </s:Header>
  <s:Body>
    <s:Fault>
       <s:Code>
         <s:Value>s:Sender</s:Value>
       </s:Code>
       <s:Reason>
        <s:Text xml:lang="en-US">The specified password is incorrect.</s:Text>
       </s:Reason>
          <s:Detail>
            <RasException
xmlns="http://schemas.datacontract.org/2004/07/Nuance.Radiology.Services"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
        <Code>4</Code> <Details>


Nuance.Radiology.Services.RasApplicationException: The specified password is incorrect.&#xD; at
Nuance.Radiology.Services.SessionService.XXXX(Int32 healthXXXX, String accXXXX, String logXXX,
String XXXX, String newXXX, Boolean adminXXX, String verXXX, String workXXX, String addXXX,
String loXX, String timeXXX)&#xD; at


   SyncInvokeXXX(Object , Object[] , Object[] )&#xD; at
System.ServiceXXXX.Dispatcher.SyncXXXXXr.Invoke(Object instance,

   Object[] inputs, Object[]&amp; outputs)&#xD; at


        System.ServiceModel.Dispatcher.DispatchOperationRuntime.InvokeBegin(MessageRpc&amp;
rpc)&#xD; =o7< at

        System.ServiceModel.Dispatcher.ImmutableDispatchRuntime.ProcessMessage5(MessageRpc&amp;
rpc)&#xD; at
```

```
        System.ServiceModel.Dispatcher.ImmutableDispatchRuntime.ProcessMessage31(MessageRpc&amp;
rpc)&#xD; at

        System.ServiceModel.Dispatcher.MessageRpc.Process(Boolean isOperationContextSet)
</Details>


        <Type>InvalidOperation</Type>

        </RasException>

             </s:Detail>

          </s:Fault>

       </s:Body>

</s:Envelope>
```


## Recommendations

Consider the following recommendations during development:

1. Code that might throw exceptions should be wrapped with the try and catch statements.
2. Send custom error messages without disclosing technical details, including information sent to log messages.
3. Avoid errors that might accidentally tip off an attacker about internal states, such as whether a file, username, or password exists.

Consider the following recommendations for healthcare providers:

1. Identify the medical devices in your network.
2. Monitor their behavior for suspicious activity and get real-time alerts.
3. Detect the level of risk exposure of your devices to take actions proactively before their security is compromised.