Dofus 2 & 3

Rétro-ingéniérie et recherche de vulnérabilité

N0x - @Bière Sécu - 07 janvier 2025

TLP:AMBER

Whoami

- DevSecOps @Icodia
- @n0xyne sur Discord
- n0x.cc

Dofus

- MMORPG Français
- Made by Ankama
- 15M joueurs
- 20+ ans

TLP:AMBER

Timeline

- **Dofus 1** : 2004 - 2009
- **Dofus 2** : 2009 - 2024
- **Dofus 3** : Décembre 2024

TLP:AMBER

Communautés RE

LÉGAL

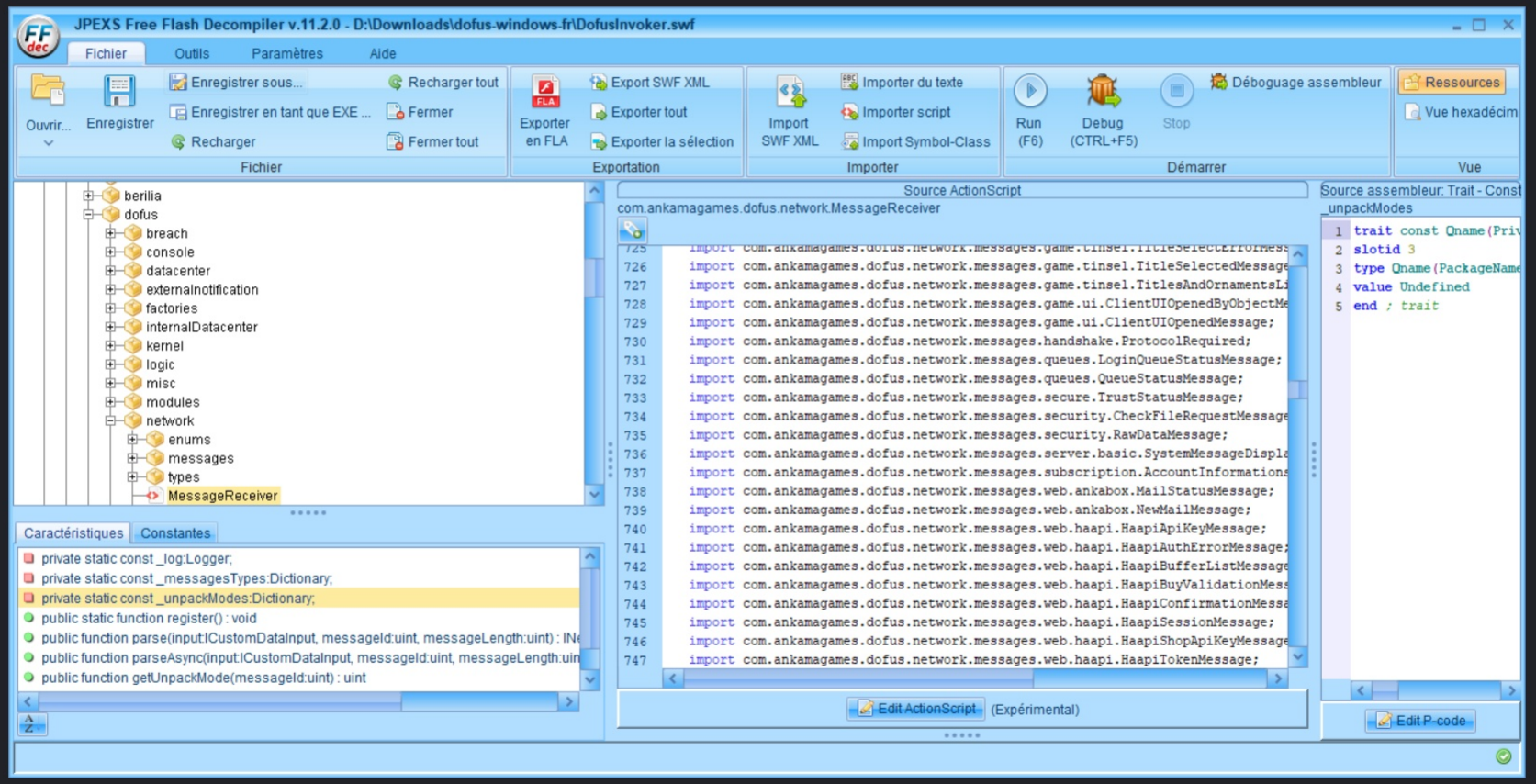
- Rétro-ingénieur
- Curieux
- Pentester
- Ankama

ILLÉGAL

- Bots
- Serveurs privé
- Hacker

TLP:AMBER

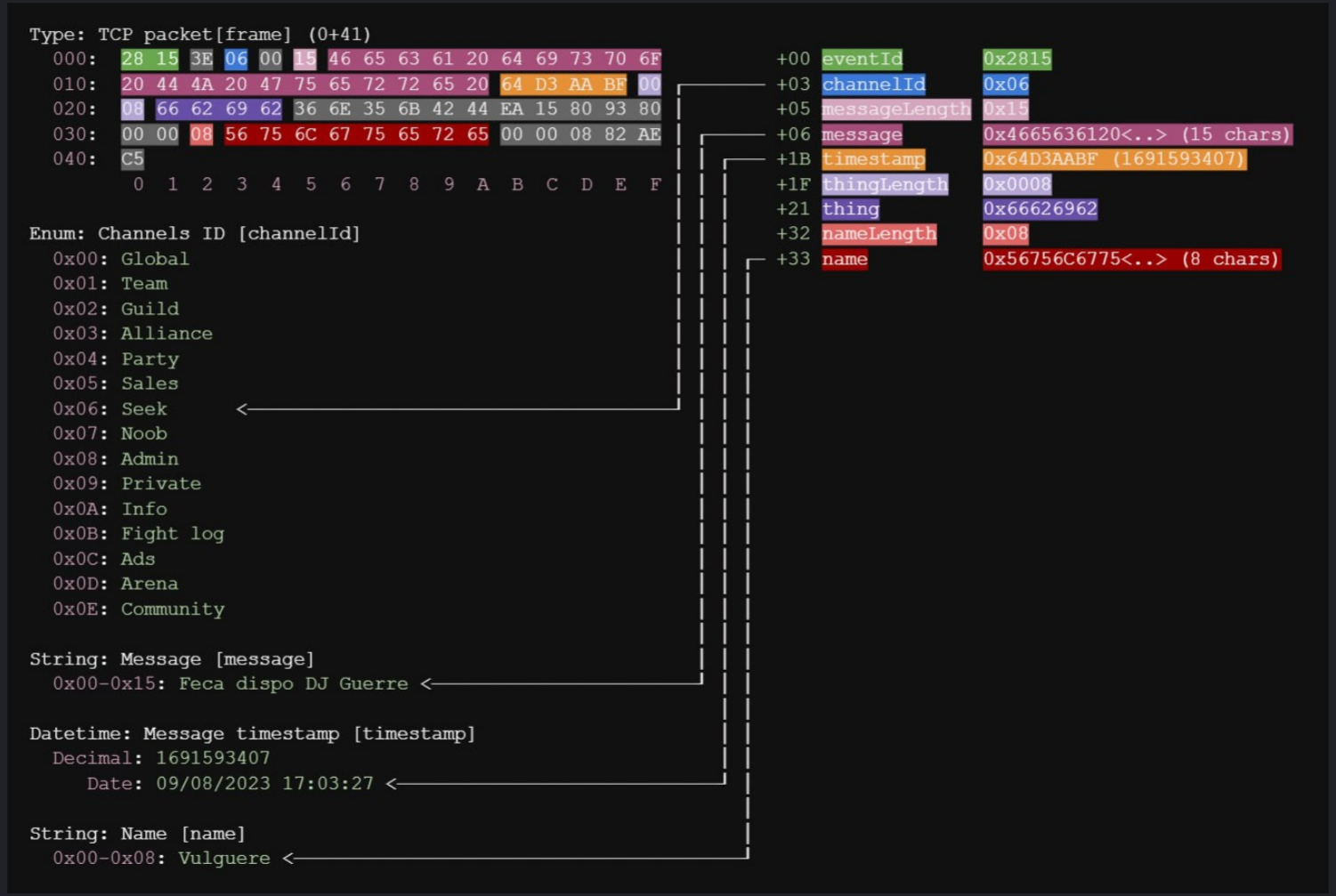
RE: Flash


JPEXS Free Flash Decompiler v.11.2.0 - D:\Downloads\dofus-windows-fr\DofusInvoker.swf
Fichier
Outils
Paramètres
Aide
Ouvrir...
Enregistrer
Enregistrer sous...
Enregistrer en tant que EXE ...
Recharger
Recharger tout
Fermer
Fermer tout
Fichier
Exporter en FLA
Export SWF XML
Exporter tout
Exporter la sélection
Exportation
Import SWF XML
Importer du texte
Importer script
Import Symbol-Class
Importer
Run (F6)
Debug (CTRL+F5)
Stop
Déboguage assembleur
Démarrer
Ressources
Vue hexadécim
Vue
berilia
dofus
breach
console
datacenter
externalnotification
factories
internalDatacenter
kernel
logic
misc
modules
network
enums
messages
types
MessageReceiver
Caractéristiques
Constantes
private static const _log:Logger;
private static const _messagesTypes:Dictionary;
private static const _unpackModes:Dictionary;
public static function register() : void
public function parse(input:ICustomDataInput, messageId:uint, messageLength:uint) : IN
public function parseAsync(input:ICustomDataInput, messageId:uint, messageLength:uin
public function getUnpackMode(messageId:uint) : uint
Source ActionScript
com.ankamagames.dofus.network.MessageReceiver
726 import com.ankamagames.dofus.network.messages.game.tinsel.TitleSelectedMessage
727 import com.ankamagames.dofus.network.messages.game.tinsel.TitlesAndOrnamentsLi
728 import com.ankamagames.dofus.network.messages.game.ui.ClientUIOpenedByObjectMe
729 import com.ankamagames.dofus.network.messages.game.ui.ClientUIOpenedMessage;
730 import com.ankamagames.dofus.network.messages.handshake.ProtocolRequired;
731 import com.ankamagames.dofus.network.messages.queues.LoginQueueStatusMessage;
732 import com.ankamagames.dofus.network.messages.queues.QueueStatusMessage;
733 import com.ankamagames.dofus.network.messages.secure.TrustStatusMessage;
734 import com.ankamagames.dofus.network.messages.security.CheckFileRequestMessage
735 import com.ankamagames.dofus.network.messages.security.RawDataMessage;
736 import com.ankamagames.dofus.network.messages.server.basic.SystemMessageDispla
737 import com.ankamagames.dofus.network.messages.subscription.AccountInformations
738 import com.ankamagames.dofus.network.messages.web.ankabox.MailStatusMessage;
739 import com.ankamagames.dofus.network.messages.web.ankabox.NewMailMessage;
740 import com.ankamagames.dofus.network.messages.web.haapi.HaapiApiKeyMessage;
741 import com.ankamagames.dofus.network.messages.web.haapi.HaapiAuthErrorMessage;
742 import com.ankamagames.dofus.network.messages.web.haapi.HaapiBufferListMessage
743 import com.ankamagames.dofus.network.messages.web.haapi.HaapiBuyValidationMess
744 import com.ankamagames.dofus.network.messages.web.haapi.HaapiConfirmationMessa
745 import com.ankamagames.dofus.network.messages.web.haapi.HaapiSessionMessage;
746 import com.ankamagames.dofus.network.messages.web.haapi.HaapiShopApiKeyMessage
747 import com.ankamagames.dofus.network.messages.web.haapi.HaapiTokenMessage;
Edit ActionScript
(Expérimental)
Source assembleur: Trait - Const _unpackModes
1 trait const Qname(Priv
2 slotid 3
3 type Qname(PackageName
4 value Undefined
5 end ; trait
Edit P-code

RE: Flash

- 4000+ messages (évènements, requêtes, réponses)
- Code "obfusqué" (noms, ids, ...)
- Librairies dépréciées depuis 10+ ans (crypto, lua, ...)
- Encore très utilisé malgré l'arrivé de Dofus 3

RE: Flash - Network



RE: Flash - Fun artifacts

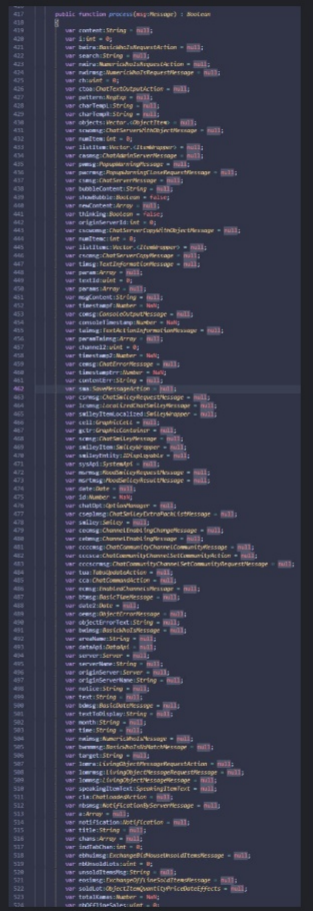
```
279         -- TODO: Huge overhead, but simple. Rewrite.
```

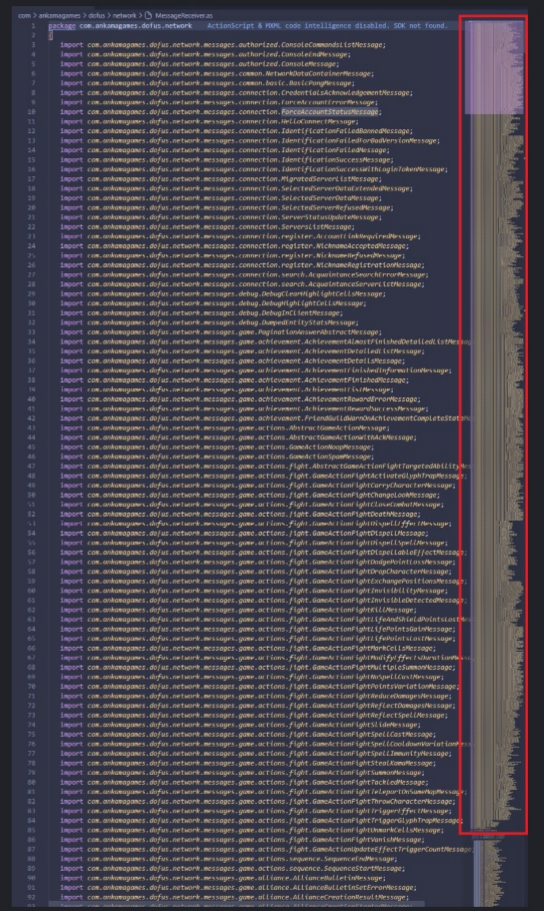
```
6   -- TODO: Fix this as soon as Alchemy team clarifies situations
```

```
313         -- TODO: Really?
314         error("namespace objects can not be resolved to actual value")
```

```
424         -- TODO: Why is this not a configurable function as with callobj?
425         --
426         -- Looks really slow, especially for
427         -- as3.class.a.b.c.new() kind of thing.
```

```
173     -- TODO: HACK! There should be a legal way to do this!
174     local mt = debug.getmetatable(assert(as3.new("String")))
```





RE: Unity

ChannelMessageEvent

```
using System;
using System.CodeDom.Compiler;
using System.Diagnostics;
using Com.Ankama.Dofus.Server.Game.Protocol.Common;
using Google.Protobuf;
using Google.Protobuf.Collections;
using Google.Protobuf.Reflection;
using Il2CppDummyDll;

namespace Com.Ankama.Dofus.Server.Game.Protocol.Chat
{
    // Token: 0x02000A85 RID: 2693
    [Token(Token = "0x2000A85")]
    [DebuggerDisplay("{ToString(),nq}")]
    public sealed class ChatChannelMessageEvent : IMessage<ChatChannelMessageEvent>, IMessage, IEquatable<ChatChanne
    {
        // Token: 0x170018C5 RID: 6341
        // (get) Token: 0x06006F8B RID: 28555 RVA: 0x00002050 File Offset: 0x00000250
        [Token(Token = "0x170018C5")]
        [DebuggerNonUserCode]
        [GeneratedCode("protoc", null)]
        public static MessageParser<ChatChannelMessageEvent> Parser
        {
            [Token(Token = "0x6006F8B")]
            [Address(RVA = "0xBDEFD0", Offset = "0xBDD5D0", VA = "0x180BDEFD0")]
            get
            {
                return null;
            }
        }

        // Token: 0x170018C6 RID: 6342
        // (get) Token: 0x06006F8C RID: 28556 RVA: 0x00002050 File Offset: 0x00000250
        [Token(Token = "0x170018C6")]
        [DebuggerNonUserCode]
        [GeneratedCode("protoc", null)]
        public static MessageDescriptor Descriptor
        {
            [Token(Token = "0x6006F8C")]
            [Address(RVA = "0xBDEEB0", Offset = "0xBDD4B0", VA = "0x180BDEEB0")]
            get
            {
                return null;
            }
        }

        // Token: 0x170018C7 RID: 6343
        // (get) Token: 0x06006F8D RID: 28557 RVA: 0x00002050 File Offset: 0x00000250
        [Token(Token = "0x170018C7")]
        [GeneratedCode("protoc", null)]
        [DebuggerNonUserCode]
        private MessageDescriptor Descriptor
        {
            [Token(Token = "0x6006F8D")]
            [Address(RVA = "0xBDF540", Offset = "0xBDDB40", VA = "0x180BDF540", Slot = "8")]
            get
            {
                return null;
```

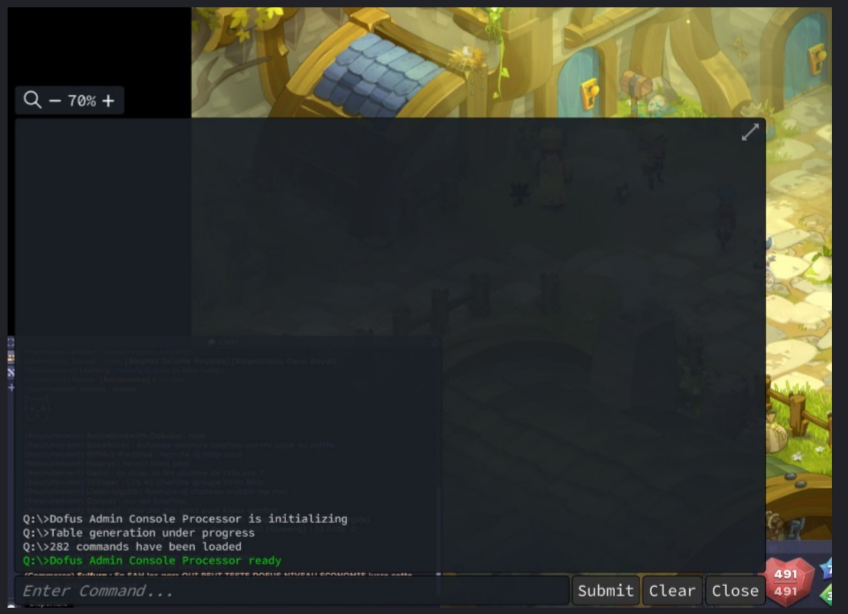
RE: Unity

- IL2CPP
- Protobuf + gRPC
- Rendu & UI custom

TLP:AMBER

RE: Unity - Outils

- dnSpy (decompiling)
- BepInEx (overlay)
- UABEA (assets export)
- Doduda (client cli)



Recherche de vulnérabilité

1. TextMeshPro
2. Injections & bypass
3. RCE One-Click

TLP:AMBER

TextMeshPro

- Racheté en 2018 par Unity et rendue propriétaire
- Par défaut sur Unity
- Intégré dans uGUI
- Bugs, ambigüitées, "features" non-documenté

Balises

Officiellement

<align>	<allcaps	<alpha
<b>	 	<color>
<cspace>	<font>	<font-weight>
<gradient>	<i>	<indent>
<line-height>	<line-indent>	<link>
<lowercase>	<margin>	<nobr>
<noparse>	<page>	<pos>
<rotate>	<s>	<size>
<smallcaps>	<space>	<sprite>
<strikethrough>	<style>	<sub>
<sup>	<u>	<uppercase>
<voffset>	<width>	

...

```
new MarkupTagDescriptor("ACTION", "action", "// <action>"),
new MarkupTagDescriptor("SLASH_ACTION", "/action", "// </action>"),
MarkupTagDescriptor.linefeed,

new MarkupTagDescriptor("CLASS", "class", "// <class>"),
new MarkupTagDescriptor("TABLE", "table", "// <table>"),
new MarkupTagDescriptor("SLASH_TABLE", "/table", "// </table>"),
new MarkupTagDescriptor("TH", "th", "// <th>"),
new MarkupTagDescriptor("SLASH_TH", "/th", "// </th>"),
new MarkupTagDescriptor("TR", "tr", "// <tr>"),
new MarkupTagDescriptor("SLASH_TR", "/tr", "// </tr>"),
new MarkupTagDescriptor("TD", "td", "// <td>"),
new MarkupTagDescriptor("SLASH_TD", "/td", "// </td>"),
MarkupTagDescriptor.linefeed,
```

POC Injection - 1/5 (16/08)

```
<mark color="#6897BB">x</mark><mark color="#F2F3F3">x</mark><mark color="#7C0002">x</mark>
```

Fix - 1/5 (16/08)

Noparse

The `<noparse>` tag creates a scope that TextMesh Pro does not parse.

This is useful for rendering text that TextMesh Pro normally interprets as a rich text tag, without disabling rich text tags.

Example:

```
Use <noparse><b></noparse> for <b>bold</b> text.
```

Use <b> for **bold** text.

Prevent parsing of some tags

```
<noparse>CONTENT</noparse>
```

TLP:AMBER

POC Injection - 2/5 (16/08)

```
</noparse><mark color="#6897BB">x</mark><mark color="#F2F3F3">x</mark><mark color="#7C0002">x</mark>
```

Fix - 2/5 (17/08)

`</`

❌

Interdit

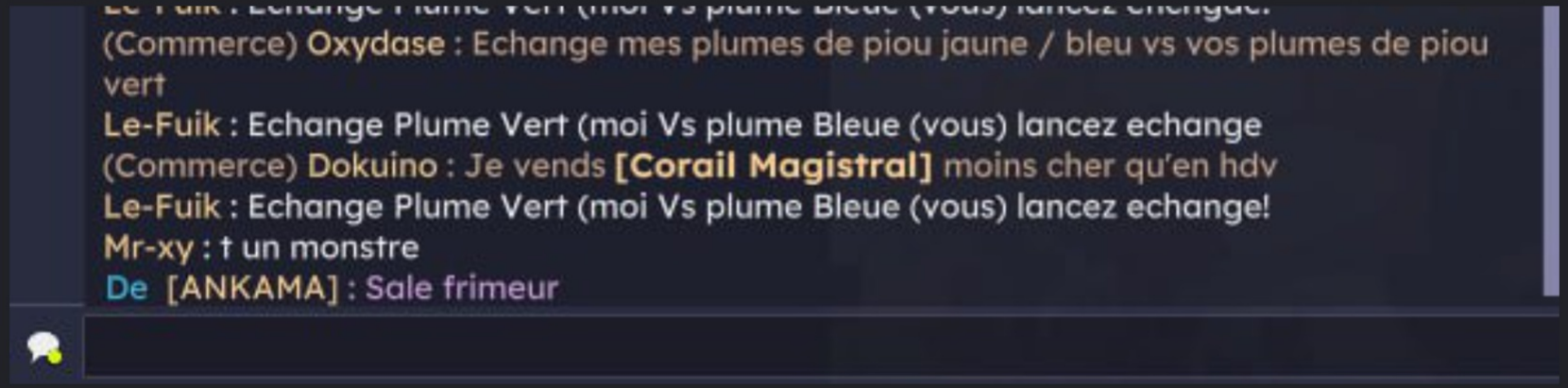
`<noparse>`

✅

Supprimé

POC Injection - 3/5 (17/08)

```
<<noparse>/noparse><mark color="#6897BB">x</mark><mark color="#F2F3F3">x</mark><mark color="#7C0002">x</mark>
```



Fix - 3/5 (19/08)

`</noparse>`

❌

Interdit

`<noparse>`

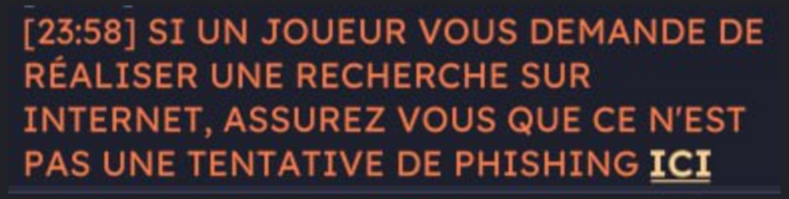
❌

Interdit

TLP:AMBER

POC Injection - 4/5 (19/08)

```
</noparse ><mark color="#6897BB">x</mark><mark color="#F2F3F3">x</mark><mark color="#7C0002">x</mark>
```



Fix - 4/5 (23/08)

<

❌

Interdit

POC Injection - 5/5 (23/08)

```
\u003cmark color="#6897BB">x\u003c/mark>\u003cmark color="#F2F3F3">x\u003c/mark>\u003cmark color="#7C0002">x\u003c/mark>
```

`\u003c` -> `<`

⬇️

```
<mark color="#6897BB">x</mark><mark color="#F2F3F3">x</mark><mark color="#7C0002">x</mark>
```

Fix - 5/5 (02/12)

<

<

>

>

POC Injection - 6/5 (05/01)

To be continued

POC RCE 1-Click

Questions