Loader-based Dynamic Software Updates for Off-the-shelf Shared Objects

July 10, 2023

Bernhard Heinloth, Peter Wägemann, and Wolfgang Schröder-Preikschat

Friedrich-Alexander-Universität Erlangen-Nürnberg
```c
#define SZ 128
char buf[SZ];

int bar(char* tmp) {
    int n = 0;
    while (*tmp != 0) {
        buf[n++] = *tmp++;
    }
    return n;
}
```
#define SZ 128
char buf[SZ];

int bar(char* tmp) {
    int n = 0;
    while (*tmp != 0) {
        buf[n++] = *tmp++;
    }
    return n;
}
```c
#define SZ 128
char buf[SZ];

int bar(char* tmp) {
    int n = 0;
    while (*tmp != 0) {
        buf[n++] = *tmp++;
    }
    return n;
}
```
```c
#define SZ 128
char buf[SZ];

int bar(char* tmp) {
    int n = 0;
    while (*tmp != 0) {
        buf[n++] = *tmp++;
    }
    return n;
}
```
#define SZ 128
char buf[SZ];

int bar(char* tmp) {
    int n = 0;
    while (*tmp != 0) {
        buf[n++] = *tmp++;
    }
    return n;
}

---

Base version:

- **bar.c**
- **bar.o**
- **x.elf v1.0.2**

Updated version:

- **bar.c**
- **bar.o**
- **x.elf v1.0.3**

---

Heinloth et al. LUCI
Dynamic Software Updates

base version

bar.c

`#define SZ 128
char buf[SZ];

int bar(char* tmp) {
    int n = 0;
    while (*tmp != 0) {
        buf[n++] = *tmp++;
    }
    return n;
}

bar.o

virtual memory

code
data
heap

updated version

bar.c

`#define SZ 128
char buf[SZ];

int bar(char* tmp){
    int n = 0;
    if (tmp != 0x0)
        while (*tmp != 0) {
            buf[n++] = *tmp++;
            if (n >= SZ)
                break;
        }
    return n;
}

bar.o

x.elf v1.0.3

inject changes

virtual memory

code
data
heap

stack

Heinloth et al.

LUCI
Dynamic Software Updates

Related Work

Existing approaches
- require changes in source code
- need further privileges to patch processes
- introduce runtime overhead
- have limitations on consecutive updates:
  - prevents broad adoption in user space

A practical DSU
- must adapt to existing build chains and package distribution
- be transparent to the user
- have no impact on runtime
- be suitable for (multiple) security fixes

Heinloth et al.

LUCI
Dynamic Software Updates

Related Work

- Existing approaches require changes in source code or modified build tools.
- They need further privileges to patch processes.
- Introduce runtime overhead.
- Have limitations on consecutive updates: prevents broad adoption in user space.

Patcher

Practical DSU for user-space application must adapt to existing build chains and package distribution.

be transparent to the user

be suitable for (multiple) security fixes.

Heinloth et al.
Dynamic Software Updates

Related Work

Existing approaches
- require changes in source code or modified build tools
- need further privileges to patch processes
- introduce runtime overhead
- have limitations on consecutive updates: prevents broad adoption in user space

Practical DSU for user-space application must
- adapt to existing build chains and package distribution
- be transparent to the user
- have no impact on runtime
- be suitable for (multiple) security fixes
Dynamic Software Updates

Related Work

Existing approaches
- require changes in source code or modified build tools
- need further privileges to patch processes
- introduce runtime overhead
- have limitations on consecutive updates: prevents broad adoption in user space

A practical DSU for user-space application must adapt to existing build chains and package distribution be transparent to the user have no impact on runtime be suitable for (multiple) security fixes

Heinloth et al.

LUCI
Dynamic Software Updates

Related Work

Existing approaches
- require changes in source code or modified build tools
- need further privileges to patch processes
- introduce runtime overhead
- have limitations on consecutive updates:
  - prevents broad adoption in user space

A practical DSU for user-space application must adapt to existing build chains and package distribution be transparent to the user have no impact on runtime be suitable for (multiple) security fixes

Heinloth et al. LUCI
Dynamic Software Updates

Related Work

Heinloth et al.
Dynamic Software Updates

Limitations of Related Work

Heinloth et al.

LUCI
Dynamic Software Updates

Limitations of Related Work

Existing approaches:
- require changes in source code or modified build tools
- need further privileges to patch processes
- introduce runtime overhead
- have limitations on consecutive updates
- prevents broad adoption in user space

A practical DSU for user-space applications must:
- adapt to existing build chains and package distribution
- be transparent to the user
- have no impact on runtime
- be suitable for (multiple) security fixes
Dynamic Software Updates

Limitations of Related Work

Existing approaches

- require changes in source code or modified build tools
- need further privileges to patch processes
- introduce runtime overhead
- have limitations on consecutive updates

→ prevents broad adoption in user space

Heinloth et al.
Dynamic Software Updates

Goal: Practical Approach

```
#define SZ 128
char buf[SZ];

int bar(char* tmp) {
    int n = 0;
    while (*tmp != 0) {
        buf[n++] = *tmp++;
    }
    return n;
}
```

```
#include <stdio.h>

int bar(char* tmp) {
    printf("%s\n", tmp);
    int n = 0;
    while (*tmp != 0) {
        buf[n++] = *tmp++;
    }
    return n;
}
```

Existing approaches:
- Require changes in source code or modified build tools.
- Need further privileges to patch processes.
- Introduce runtime overhead.
- Have limitations on consecutive updates, preventing broad adoption in user space.

A practical DSU for user-space applications must:
- Adapt to existing build chains and package distribution.
- Be transparent to the user and have no impact on runtime.
- Be suitable for (multiple) security fixes.

Heinloth et al.
Dynamic Software Updates

**Goal: Practical Approach**

```
#define SZ 128
char buf[SZ];

int bar(char* tmp) {
    int n = 0;
    while (*tmp != 0) {
        buf[n++] = *tmp++;
    }
    return n;
}
```

```
#define SZ 128
char buf[SZ];

int bar(char* tmp) {
    int n = 0;
    if (tmp != 0x0)
        while (*tmp != 0) {
            buf[n++] = *tmp++;
            if (n >= SZ)
                break;
        }
    return n;
}
```

**Distributor**

**base version**
- `bar.c`
- `bar.o`
- `x.elf v1.0.2`

**updated version**
- `bar.c`
- `bar.o`
- `x.elf v1.0.3`

**virtual memory**
- code
- data
- heap
- stack

**Existing approaches**
- require changes in source code
- need further privileges to patch processes
- introduce runtime overhead
- have limitations on consecutive updates

**Heinloth et al.**

**LUCI**
Dynamic Software Updates

Goal: Practical Approach

```
#define SZ 128
char buf[SZ];

int bar(char* tmp) {
    int n = 0;
    while (*tmp != 0) {
        buf[n++] = *tmp++;
    }
    return n;
}
```

```
bar.o
7f454c460201010000000000
0000000001003e0001000000
000000000000000000000000
00000000d002000000000000
000000004000000000004000
0d000c00f30f1efa554889e5
48897de8c745fc00000000eb
25488b45e8488d5001488955
e88b55fc8d4a01894dfc0fb6
084863c2488d150000000088
0c10488b45e80fb60084c075
d08b45fc5dc3004743433a20
285562756e747520392e342e
x.elf
v1.0.2
```

```
#define SZ 128
char buf[SZ];

int bar(char* tmp) {
    int n = 0;
    if (tmp != 0x0)
        while (*tmp != 0) {
            buf[n++] = *tmp++;
            if (n >= SZ)
                break;
        }
    return n;
}
```

```
bar.o
7f454c460201010000000000
0000000001003e0001000000
000000000000000000000000
000000005d000c00f30f1efa554889e5
48897de8c745fc0000000048837de800743beb2b488b45e8488d5001488955e88b55fc8d4a01894dfc0fb6084863c2488d1500000000880c10837dfc7f7f0d488b45e80fb684c075caeb01908b45fc5d3c0047837dfc
x.elf
v1.0.3
```

Existing approaches:
n. require changes in source code
n. need further privileges to patch processes
n. introduce runtime overhead
n. have limitations on consecutive updates

Practical DSU for user-space application must:
- adapt to existing build chains and package distribution
- be transparent to the user
- have no impact on runtime
- be suitable for (multiple) security fixes
Dynamic Software Updates

Bar.c
```c
#define SZ 128
char buf[SZ];
int bar(char* tmp) {
    int n = 0;
    while (*tmp != 0) {
        buf[n++] = *tmp++;
    }
    return n;
}
```

Bar.o
```
7f454c460201010000000000
0000000001003e0001000000
000000000000000000000000
00000000d002000000000000
000000004000000000004000
0d000c00f30f1efa554889e5
48897de8c745fc00000000eb
25488b45e8488d5001488955
e88b55fc8d4a01894dfc0fb6
084863c2488d150000000088
0c10488b45e80fb600
```

x.elf
```
v1.0.2
```

A **practical DSU** for user-space application must

- adapt to existing build chains and package distribution
- be transparent to the user
- have no impact on runtime
- be suitable for (multiple) security fixes

Heinloth et al.
User-Space Applications

App

Application
User-Space Applications

Application
using

- standard library
User-Space Applications

Application using
- standard library
- cryptography
- data (de-)compression
- parsing
- ...

Dynamically loaded modules and its dependencies

Compatibility
- PCRE
- ZLIB
- EXPAT
- OPENSSL
- LIBXCRYPT
- GLIBC

RTLD fixing
- relocations
- static relocations
- alias
- page fault handler

CVEs with CVSS v2 score
- CVE-2022-22827 denial of service
- CVE-2022-25314 denial of service
- CVE-2021-45960 denial of service
- CVE-2022-25313 DoS [code exec?]
- CVE-2022-22826 denial of service
- CVE-2022-23990 denial of service
- CVE-2022-22825 denial of service
- CVE-2022-40674 DoS [code exec?]
- CVE-2022-25236 code execution
- CVE-2022-25235 code execution
- CVE-2022-22822 denial of service
- CVE-2021-46143 denial of service
- CVE-2022-23852 denial of service
- CVE-2022-22823 denial of service
- CVE-2022-22824 denial of service

CVE-2022-22822.patch
CVE-2022-23852.patch
CVE-2022-22823.patch
CVE-2022-22824.patch
CVE-2022-23852.patch

RTLD loading shared object
- interpreter
- neededSize
- if
- neededSize += keep;
- if
- keep = XML_CONTEXT_BYTES;
- if
- keep = INT_MAX
- if
- XML_ERROR_NO_MEMORY
- return
- if
- m_errorCode
- static relocations
- EXPAT_SAFE_PTR_DIFF(parser->...}
- XML_Parser
- xmlparse
- keep = b
- if
- m_errorCode
- static relocations
- EXPAT_SAFE_PTR_DIFF(parser->...}
- XML_Parser
- xmlparse
- keep = b
- if
- m_errorCode
- static relocations
- EXPAT_SAFE_PTR_DIFF(parser->...}
- XML_Parser
- xmlparse
- keep = b
- if
-..
User-Space Applications

Apache HTTP Server using
- EXPAT
- GLIBC
- LIBXCrypt
- OpenSSL
- PCRE
- ZLIB

(+ dynamically loaded modules and its dependencies)
Apache HTTP Server using

- EXPAT
- GLIBC
- LIBXCRYPT
- OpenSSL
- PCRE
- ZLIB

(+ dynamically loaded modules and its dependencies)
### User-Space Applications

**Fixed Expat Security Vulnerabilities in 2022**

<table>
<thead>
<tr>
<th>CVE ID</th>
<th>Impact</th>
<th>CVSS v2/v3</th>
<th>Fixed Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2021-45960</td>
<td>denial of service</td>
<td>9.0 / 8.8</td>
<td>2.4.3 (Jan. 16, 2022)</td>
</tr>
<tr>
<td>CVE-2021-46143</td>
<td>denial of service</td>
<td>6.8 / 7.8</td>
<td>2.4.3</td>
</tr>
<tr>
<td>CVE-2022-22822</td>
<td>denial of service</td>
<td>7.5 / 9.8</td>
<td>2.4.3</td>
</tr>
<tr>
<td>CVE-2022-22823</td>
<td>denial of service</td>
<td>7.5 / 9.8</td>
<td>2.4.3</td>
</tr>
<tr>
<td>CVE-2022-22824</td>
<td>denial of service</td>
<td>7.5 / 9.8</td>
<td>2.4.3</td>
</tr>
<tr>
<td>CVE-2022-22825</td>
<td>denial of service</td>
<td>6.8 / 8.8</td>
<td>2.4.3</td>
</tr>
<tr>
<td>CVE-2022-22826</td>
<td>denial of service</td>
<td>6.8 / 8.8</td>
<td>2.4.3</td>
</tr>
<tr>
<td>CVE-2022-22827</td>
<td>denial of service</td>
<td>6.8 / 8.8</td>
<td>2.4.3</td>
</tr>
<tr>
<td>CVE-2022-23852</td>
<td>denial of service</td>
<td>7.5 / 9.8</td>
<td>2.4.4 (Jan. 30, 2022)</td>
</tr>
<tr>
<td>CVE-2022-23990</td>
<td>denial of service</td>
<td>5.0 / 7.5</td>
<td>2.4.4</td>
</tr>
<tr>
<td>CVE-2022-25235</td>
<td>code execution</td>
<td>7.5 / 9.8</td>
<td>2.4.5 (Feb. 18, 2022)</td>
</tr>
<tr>
<td>CVE-2022-25236</td>
<td>code execution</td>
<td>7.5 / 9.8</td>
<td>2.4.5 / 2.4.7 (March 4, 2022)</td>
</tr>
<tr>
<td>CVE-2022-25313</td>
<td>DoS [code exec?]</td>
<td>4.3 / 6.5</td>
<td>2.4.5 / 2.4.6 (Feb. 20, 2022)</td>
</tr>
<tr>
<td>CVE-2022-25314</td>
<td>denial of service</td>
<td>5.0 / 7.5</td>
<td>2.4.5</td>
</tr>
<tr>
<td>CVE-2022-25315</td>
<td>DoS [code exec?]</td>
<td>7.5 / 9.8</td>
<td>2.4.5</td>
</tr>
<tr>
<td>CVE-2022-40674</td>
<td>DoS [code exec?]</td>
<td>- / 8.1</td>
<td>2.4.9 (Sept. 20, 2022)</td>
</tr>
<tr>
<td>CVE-2022-43680</td>
<td>DoS [code exec?]</td>
<td>- / 7.5</td>
<td>2.5.0 (Oct. 25, 2022)</td>
</tr>
</tbody>
</table>
User-Space Applications

Apache HTTP Server using

- EXPAT
- GLIBC
- LIBXCRYPT
- OpenSSL
- PCRE
- ZLIB

(+ dynamically loaded modules and its dependencies)

CVEs with CVSS v2 score ≥ 7.0
User-Space Applications

Vulnerabilities in Apache2 since 2010

Apache HTTP Server using

- EXPAT
- GLIBC
- LIBXCrypt
- OpenSSL
- PCRE
- Zlib

(+ dynamically loaded modules and its dependencies)

CVEs with CVSS v2 score ≥ 7.0
User-Space Applications

Apache HTTP Server using

- EXPAT
- GLIBC
- LIBXCRYPT
- OpenSSL
- PCRE
- ZLIB

(+ dynamically loaded modules and its dependencies)

CVEs with CVSS v2 score ≥ 7.0

RTLD has meta information and data (de-)compression, cryptography, and interpreter loading shared object.

app code

lib code

data

app data

lib data

RTLD

app.elf

app.elf

xmlparse

parser = INT_MAX + 2067, 11

neededSize += keep;

if (keep > XML_CONTEXT_BYTES)

keep = XML_CONTEXT_BYTES;

/*

Detect overflow and -2067, 6

*/

if @@

prevent.

expat

expat

/*
No structural changes in security fixes

Library functions eventually gain access to process virtual memory

RTLD has meta information and a same interface (API)

Adapt dynamic loading of libraries in RTLD for updates

libx.so

meta
code
ro
relro
data
bss

app.o

code
data
meta

CVE IDs:

- CVE-2022-22826: Denial of service
- CVE-2022-23990: Denial of service
- CVE-2022-22827: Denial of service
- CVE-2022-40674: DoS [code exec?]
- CVE-2022-25314: Denial of service
- CVE-2022-22822: Denial of service
- CVE-2022-22823: Denial of service
- CVE-2022-22825: Denial of service
- CVE-2022-43680: DoS [code exec?]

Dynamically loaded modules and its dependencies

Compatability

Analyze and modify event

ZLIB
PCRE
Parsing
Data (de-)compression
LIBXCRIPT
GLIBC
Cryptography
EXPAT
Standard library

Load non-writable sections

interpreter

Return

Detect neededSize
if neededSize += keep;
if (keep > XML_CONTEXT_BYTES)
    return XML_ERROR_NO_MEMORY;
else
    keep = (keep - XML_CONTEXT_BYTES) + neededSize;
    parser->... = EXPAT_SAFE_PTR_DIFF(parser->...,
        XML_ParserContextGet(parser) + (parser->...);
    return 0;

xmlparse

Operating system

Page Fault

RTLD fixing

Update handler.

Virtual memory

CVE IDs with CVSS v2 score:

- CVE-2021-45960: Denial of service (CVSS score: 2.4.3, Fixed Release: 2.4.3 (Jan. 16, 2022))
- CVE-2022-22827: Denial of service (CVSS score: 2.4.3, Fixed Release: 2.4.3 (Jan. 16, 2022))
- CVE-2022-22823: Denial of service (CVSS score: 2.4.3, Fixed Release: 2.4.3 (Jan. 16, 2022))
- CVE-2022-40674: DoS [code exec?] (CVSS score: 2.4.5, Fixed Release: 2.5.0 (Oct. 25, 2022))
- CVE-2022-25236: Code execution (CVSS score: 2.4.5, Fixed Release: 2.4.5 / 2.4.6 (Feb. 20, 2022))
- CVE-2022-25235: Code execution (CVSS score: 2.4.4 / 2.4.3 (Jan. 30, 2022))
RTLD has meta information and code changes only for updated libraries. Dynamic loading of libraries in RTLD requires structural changes in the security fixes for the affected libraries.

CVEs with CVSS v2 score:

- CVE-2022-22826: denial of service (impact = 8.8/
- CVE-2022-22827: denial of service (impact = 7.5/
- CVE-2022-25236: code execution (impact = 7.5/
- CVE-2022-25314: denial of service (impact = 7.5/
- CVE-2022-25313: DoS (impact = 7.5/
- CVE-2022-40674: DoS (impact = 7.5/
- CVE-2021-45960: denial of service (impact = 6.5/
- CVE-2022-23852: denial of service (impact = 9.8/
- CVE-2022-22825: denial of service (impact = 9.8/
- CVE-2022-22824: denial of service (impact = 9.8/
- CVE-2022-22823: denial of service (impact = 9.8/
- CVE-2022-22822: denial of service (impact = 9.8/

RTLD fixing dynamically loaded modules and its dependencies.

compatibility issues between different platforms.

Listing: XML parsing data (de-)compression, LUCI

if (neededSize > XML_CONTEXT_BYTES)

keep = XML_CONTEXT_BYTES;

++

-2067,6

return

Detect

overflow -2067,6

@@

return

prevent

XML_ERROR_NO_MEMORY

integer

and

*/

b

XML_GetBuffer

{/}

/*

a

parser

+2067,11

NULL

expat

expat

+2067,11

INT_MAX

/
Heinloth et al.

Dynamic Library Linkage

---

app.o
- code
- data
- meta

libx.so
- meta
- code
- data
- ro
- relro
- data
- bss

app.elf
- meta
- code
- data

---

CVEs with CVSS v2 score

CVE-2022-25313 DoS [code exec?] 9.8
CVE-2021-46143 denial of service 4.3
CVE-2022-22824 denial of service
CVE-2022-23990 denial of service

RTLD has meta information and only code changes
same interface (API)
adapt dynamic loading of libraries in RTLD for updates

libx.so
- ro
- relro
- data
- bss

app.elf
- meta
- code
- data

---

dynamic loaded modules and its dependencies
compatibility
analyze
modify event
ZLIB...
PCRE...
OPENSSL...
GLIBC...
EXPAT...

---

page fault handler.

---

r/ w  r  r  r/ w  r

---

CVE-2022-23852 denial of service
CVE-2022-22825 denial of service
CVE-2022-22823 denial of service
CVE-2022-43680 DoS [code exec?] - /
CVE-2022-22822 denial of service
CVE-2022-25315 DoS [code exec?] 8.8
CVE-2022-25236 code execution 7.5
no structural changes in security fixes
dynamically loaded modules and its dependencies

---

App code
App data
Libx.so

- Meta
- Code
- Data
- RO
- RO
- Data
- BSS

needed

Interpreter

RTLD
Library Linkage

app.o
- code
- data
- meta

libx.so
- meta
- code
- ro
- relro
- data
- bss

app.elf
- meta
- code
- data

RTLD

virtual memory
- static relocations
- RTLD fixing
- dyn. relocations
- static relocations

CVE ID Impact CVSS v2/v3 Fixed Release
- CVE-2022-22826 denial of service
  - CVSS 7.5
  - 2.4.3 (Sept. 20, 2022)
- CVE-2022-25315 DoS [code exec?]
  - CVSS 7.5
  - 2.4.9 (2022)
- CVE-2021-45960 denial of service
  - CVSS 7.5
  - 2.4.5 (Feb. 18, 2022)
- CVE-2022-40674 DoS [code exec?] -
  - CVSS 7.5
  - 2.4.3 (2022)
- CVE-2022-25314 denial of service
  - CVSS 7.5
  - 2.4.3 (2022)
- CVE-2022-22825 denial of service
- CVE-2022-22827 denial of service
  - CVSS 7.5
  - 9.0 (2022)
- CVE-2022-22822 denial of service
  - CVSS 7.5
  - 8.8 (2022)
- CVE-2022-25236 code execution
  - CVSS 7.5
  - 9.8 (2022)
- CVE-2022-25235 code execution
  - CVSS 7.5
  - 2.4.5 / 2.4.7 (2022)
- CVE-2021-46143 denial of service
- CVE-2022-43680 DoS [code exec?]
- CVE-2022-23852 denial of service
  - CVSS 6.8
  - 2.4.4 (2022)
- CVE-2022-23990 denial of service
- CVE-2022-22824 denial of service
Approach
- RTLD has meta information and access to process virtual memory
- RTLD has meta information and access to process virtual memory
- library functions eventually \textit{return}
- RTLD has meta information and access to process virtual memory
- library functions eventually return
- no structural changes in security fixes
  - same interface (API)
  - only code changes
Luci Approach

CVE-2022-23852.patch

--- a/expat/lib/xmlparse.c
+++ b/expat/lib/xmlparse.c
@@ -2067,6 +2067,11 @@ XML_GetBuffer(XML_Par...
     keep = (int)EXPAT_SAFE_PTR_DIFF(parser->...}
     if (keep > XML_CONTEXT_BYTES)
     keep = XML_CONTEXT_BYTES;
+    /* Detect and prevent integer overflow */
+    if (keep > INT_MAX - neededSize) {
+        parser->m_errorCode = XML_ERROR_NO_MEMORY;
+        return NULL;
+    }
     neededSize += keep;
 #endif /* defined XML_CONTEXT_BYTES */
     if (neededSize
Loader-based Dynamic Updates

LUCI Approach

CVE-2022-23852.patch
--- a/expat/lib/xmlparse.c
+++ b/expat/lib/xmlparse.c
@@ -2067,6 +2067,11 @@ XML_GetBuffer(XML_Par...
     keep = (int)EXPAT_SAFE_PTR_DIFF(parser->...
     if (keep > XML_CONTEXT_BYTES)
         keep = XML_CONTEXT_BYTES;
+    /* Detect and prevent integer overflow */
+    if (keep > INT_MAX - neededSize) {
+        parser->m_errorCode = XML_ERROR_NO_MEMORY;
+        return NULL;
+    }
+    neededSize += keep;
#endif /* defined XML_CONTEXT_BYTES */
if (neededSize
Loader-based Dynamic Updates

Luci Approach

libx.so
- meta
- code
- ro
- data
- bss

LUCI
- analyze
- compatibility

RTLD has meta information and code changes.
No structural changes in security fixes.
Library functions eventually needed.

CVEs with CVSS v2 score:
- CVE-2022-25315 DoS [code exec?]
- CVE-2021-46143 denial of service
- CVE-2022-22826 denial of service
- CVE-2022-22824 denial of service
- CVE-2022-22825 denial of service
- CVE-2022-43680 DoS [code exec?]
- CVE-2022-25236 code execution
- CVE-2022-40674 DoS [code exec?]
- CVE-2022-22827 denial of service
- CVE-2022-23852 denial of service
- CVE-2022-22823 denial of service
- CVE-2021-45960 denial of service
- CVE-2022-22822 denial of service
- CVE-2022-25313 DoS [code exec?]
- CVE-2022-23990 denial of service
- CVE-2022-25314 denial of service
- CVE-2022-22821 denial of service
- CVE-2022-25316 denial of service

CVE-IDs and Impact:
- CVE-ID: Impact
- CVSS v2
- CVSS v3
- Fixed Release

Example:
- CVE-2022-22826: Denial of service (DoS)
- CVE-2022-25315: Denial of service (DoS) [code exec?]
- CVE-2022-43680: Denial of service (DoS) [code exec?]
- CVE-2022-23852: Denial of service
- CVE-2022-22827: Denial of service
- CVE-2022-22823: Denial of service
- CVE-2021-45960: Denial of service
- CVE-2022-22822: Denial of service
- CVE-2022-25313: Code execution
- CVE-2022-23990: Denial of service
- CVE-2022-25314: Denial of service
- CVE-2022-22821: Denial of service
- CVE-2022-25316: Denial of service

Remark:
- Multi-update
- Domains
- Reuse
- RTLD fixing
- dyn. relocations
- static relocations
- RTLD loading shared object
- sections
- writable
- read
- recompress
- ZLIB
- PCRE
- ...
Luci Approach

Heinloth et al.

Loader-based Dynamic Updates

virtual memory

load non-writable sections

app.o

libx.so

app.elf

virtual memory

app data

lib data

code

data

meta

code

data

meta

code

data

ro

rx

rw

r

rw

r

rw
Luci Approach

Loader-based Dynamic Updates

app.elf

app.o

libx.so

virtual memory

alias writable sections

Heinloth et al.
Luci Approach

Loader-based Dynamic Updates

virtual memory

update
relocations

Heinloth et al.
Luci Approach

virtual memory

page fault handler

app.o

code

data

meta

libx.so

meta

code

ro

data

bss

app.elf

meta

code

data

Luci
Advantages of the LUCI Approach

- comparatively simple and safe
- no quiescence required
- agnostic to programming language and build tools
- no overhead during runtime
- not requiring any additional permissions
- arbitrary update sequence
Advantages of the LUCI Approach

- comparatively simple and safe
Advantages of the LUCI Approach

- comparatively simple and safe
- no quiescence required
Advantages of the LUCI Approach

- comparatively simple and safe
- no quiescence required
- agnostic to programming language and build tools
Advantages of the LUCI Approach

- comparatively simple and safe
- no quiescence required
- agnostic to programming language and build tools
- no overhead during runtime
Advantages of the Luci Approach

- comparatively simple and safe
- no quiescence required
- agnostic to programming language and build tools
- no overhead during runtime
- not requiring any additional permissions
Advantages of the LUCI Approach

- comparatively simple and safe
- no quiescence required
- agnostic to programming language and build tools
- no overhead during runtime
- not requiring any additional permissions
- arbitrary update sequence
Implementation of Luci

- dynamic linker/loader (RTLD)
- basic *glibc* compatibility
- tracks file modifications of loaded shared objects
Implementation of Luci

- dynamic linker/loader (RTLD)
- basic glibc compatibility
- tracks file modifications of loaded shared objects
  - automatic compatibility check:
    - identical writable segment
    - unchanged initialization routines
    - no structural changes
Implementation of Luci

- dynamic linker/loader (RTLD)
- basic glibc compatibility
- tracks file modifications of loaded shared objects
  - automatic compatibility check:
    - identical writable segment → ELF / DWARF
    - unchanged initialization routines → ELF
    - no structural changes → ELF / DWARF
Implementation of LUCI

- dynamic linker/loader (RTLD)
- basic glibc compatibility
- tracks file modifications of loaded shared objects
  - automatic compatibility check:
    - identical writable segment \(\rightarrow\) ELF / DWARF
    - unchanged initialization routines \(\rightarrow\) ELF
    - no structural changes \(\rightarrow\) ELF / DWARF
  - on compatible library:
    1. loading to an unused memory area in process
    2. applying relocations (e.g., .data.rel.ro)
    3. updating all Global Offset Table entries referring to the changed library
    4. disabling old code segment (with some delay)
Implementation of LUCI

- dynamic linker/loader (RTLD)
- basic glibc compatibility
- tracks file modifications of loaded shared objects
  - automatic compatibility check:
    - identical writable segment $\rightarrow$ ELF / DWARF
    - unchanged initialization routines $\rightarrow$ ELF
    - no structural changes $\rightarrow$ ELF / DWARF
- on compatible library:
  1. loading to an unused memory area in process
  2. applying relocations (e.g., .data.rel.ro)
  3. updating all Global Offset Table entries referring to the changed library
  4. disabling old code segment (with some delay)
- for incompatible library:
  1. notify user (IPC)
  2. resume with old version
Evaluation
**EXPAT XML PARSER Version 2**

- widely used
  - e.g., Chromium, Cmake, GDB, Git, Firefox, LibreOffice, PHP, Python, ...
- 27 releases (since 2006)
- 29 CVEs (since 2012)
Evaluation

**EXPAT XML PARSER Version 2**

- widely used
  - e.g., Chromium, Cmake, GDB, Git, Firefox, LibreOffice, PHP, Python, ...
- 27 releases (since 2006)
- 29 CVEs (since 2012)

→ *vanilla* build of each release

- from official source
- with default configuration and tools (./buildconf.sh ; make)
- no artifacts from previous builds
- using minimal Debian Bullseye environment
<table>
<thead>
<tr>
<th>Version</th>
<th>Updatable</th>
<th>Restart</th>
<th>Compatible Change</th>
<th>Incompatible Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>v2.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.0.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.1.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.2.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.2.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.2.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.2.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.2.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.2.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.2.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.2.7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.2.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.2.9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.2.10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.3.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.4.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.4.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.4.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.4.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.4.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.4.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.4.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.4.7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.4.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.4.9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v2.5.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>section</td>
<td>V2.0.0</td>
<td>V2.0.1</td>
<td>V2.1.0</td>
<td>V2.2.0</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>.note</td>
<td>-</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
</tbody>
</table>
## Luci Compatibility Analysis

### (vanilla) EXPAT

| section | V2.0.0 | V2.0.1 | V2.1.0 | V2.1.1 | V2.2.0 | V2.2.1 | V2.2.2 | V2.2.3 | V2.2.4 | V2.2.5 | V2.2.6 | V2.2.7 | V2.2.8 | V2.2.9 | V2.2.10 | V2.3.0 | V2.4.0 | V2.4.1 | V2.4.2 | V2.4.3 | V2.4.4 | V2.4.5 | V2.4.6 | V2.4.7 | V2.4.8 | V2.4.9 | V2.5.0 |
|---------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| .note   | -     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     |
| .init   | -     |       |       |       |       |       |       |       |       |       |       |       |       |       |       |       |       |       |       |       |       |       |       |       |       |       |       |       |

- ○: compatible change
- ●: incompatible change

---

Heinloth et al.
# Luci Compatibility Analysis

## (vanilla) Expat

| section | V2.0.0 | V2.0.1 | V2.1.0 | V2.2.0 | V2.2.1 | V2.2.2 | V2.2.3 | V2.2.4 | V2.2.5 | V2.2.6 | V2.2.7 | V2.2.8 | V2.2.9 | V2.2.10 | V2.3.0 | V2.4.0 | V2.4.1 | V2.4.2 | V2.4.3 | V2.4.4 | V2.4.5 | V2.4.6 | V2.4.7 | V2.4.8 | V2.4.9 | V2.5.0 |
|---------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| .note   | -     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     |
| .init   | -     | -     |       |       |       |       | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     |
| .text   | -     | -     |       |       |       |       |       | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     |
| .rodata | -     | -     |       |       |       |       |       |       | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     |
| .relro  | -     | -     |       |       |       |       |       |       | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     |
| .data   | -     | -     |       |       | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     |
| .bss    | -     | -     |       |       | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     |
| .debug  | -     | -     |       |       | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     | O     |

- ○: compatible change
- ●: incompatible change
### Luci Compatibility Analysis

| section | V2.0.0 | V2.0.1 | V2.1.0 | V2.2.0 | V2.2.1 | V2.2.2 | V2.2.3 | V2.2.4 | V2.2.5 | V2.2.6 | V2.2.7 | V2.2.8 | V2.2.9 | V2.2.10 | V2.3.0 | V2.4.0 | V2.4.1 | V2.4.2 | V2.4.3 | V2.4.4 | V2.4.5 | V2.4.6 | V2.4.7 | V2.4.8 | V2.4.9 | V2.5.0 |
|---------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| .note   | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      |
| .init   | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      |
| .text   | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      |
| .rodata | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      |
| .relro  | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      |
| .data   | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      |
| .bss    | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      |
| .debug  | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      | –      |

**Updatable:**

- ✓ compatible change
- ☠ incompatible change

Note: This table provides a visual representation of compatibility changes across different versions of the `.note`, `.init`, `.text`, `.rodata`, `.relro`, `.data`, `.bss`, and `.debug` sections. The table uses symbols to indicate whether changes are compatible or incompatible across versions.
## Luci Compatibility Analysis

### (vanilla) EXPAT

### Section Compatibility

| Section | V2.0.0 | V2.0.1 | V2.1.0 | V2.1.1 | V2.2.0 | V2.2.1 | V2.2.2 | V2.2.3 | V2.2.4 | V2.2.5 | V2.2.6 | V2.2.7 | V2.2.8 | V2.2.9 | V2.2.10 | V2.3.0 | V2.4.0 | V2.4.1 | V2.4.2 | V2.4.3 | V2.4.4 | V2.4.5 | V2.4.6 | V2.4.7 | V2.4.8 | V2.4.9 | V2.5.0 |
|---------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| .note   | -      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      |
| .init   | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      |
| .text   | -      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      |
| .rodata | -      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      |
| .relro  | -      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      | O      |
| .data   | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      |
| .bss    | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      |
| .debug  | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      | -      |

### Updatable

- X: Incompatible change
- ✓: Compatible change

| Updatable | X | X | ✓ | X | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

- compatible change
- incompatible change

---

Heinloth et al.
## Luci Compatibility Analysis

### (vanilla) EXPAT

| section | V2.0.0 | V2.0.1 | V2.1.0 | V2.2.0 | V2.2.1 | V2.2.2 | V2.2.3 | V2.2.4 | V2.2.5 | V2.2.6 | V2.2.7 | V2.2.8 | V2.2.9 | V2.2.10 | V2.3.0 | V2.4.0 | V2.4.1 | V2.4.2 | V2.4.3 | V2.4.4 | V2.4.5 | V2.4.6 | V2.4.7 | V2.4.8 | V2.4.9 | V2.5.0 |
|---------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| .note   | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     |
| .init   | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     |
| .text   | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     |
| .rodata | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     |
| .relro  | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     |
| .data   | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     |
| .bss    | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     |
| .debug  | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     | -     |

### compatible change

- O

### incompatible change

- X

### Restart

- incompatible change

### Updatable

- O

### Notes

- f f f f f f f f f f f f f f f f f f f f f f f f f f

- incompatible change

- updatable

- compatible change

- O

- incompatible change

- X

### Restart

- incompatible change

### Updatable

- O

- compatible change
EXPAT test suite

- good coverage
- well-maintained
TEST APPLICATION

(vanilla) EXPAT

EXPAT test suite

- good coverage
- well-maintained

\{ good evaluation target for dynamic updating releases \}
Test Application

EXPAT test suite

- good coverage
- well-maintained

\[ \text{good evaluation target for} \quad \text{dynamic updating releases} \]

Test application

- using latest test suite from \textbf{EXPAT v2.5.0} release
- version-based skipping of incompatible / fatal tests (e.g., causing segfault)
- running in endless loop
EXPAT test suite

- good coverage
- well-maintained
  
  \[
  \begin{aligned}
  & \text{good evaluation target for} \\
  & \text{dynamic updating releases}
  \end{aligned}
  \]

Test application

- using latest test suite from \textbf{EXPAT v2.5.0} release
- version-based skipping of incompatible / fatal tests (e.g., causing segfault)
- running in endless loop
- \textit{no adjustments for dynamic updates or whatsoever!}
Test Application

Testcases successful failed skipped

successively applied dynamic updates
(out of 26) releases dynamically updated with up to 10 consecutive updates incompatible releases reported consistent test results no run time overhead no inconsistent state

Heinloth et al. LUCI
Test Application with LUCI Dynamic Updates

(vanilla) EXPAT

Testcases

restart

17 (out of 26) releases dynamically updated with up to 10 consecutive updates incompatible releases reported consistent test results no run time overhead no inconsistent state

Heinloth et al.

Luci
Test Application with LUCI Dynamic Updates

Heinloth et al.
Test Application with Luci Dynamic Updates

- **17** (out of **26**) releases dynamically updated
  - with up to **10** consecutive updates
  - incompatible releases reported
- consistent test results
- no run time overhead
- no inconsistent state

**Heinloth et al.**
What about binary distributed libraries?
What about binary distributed libraries?

- backtesting *EXPAT* shared objects from Debian Buster packages
  - from Debian snapshot archive
  - simulate previous real-world package updates
  - including development builds
  - excluding debug symbols
## LucI Compatibility Analysis

### EXPAT from Debian Buster

<table>
<thead>
<tr>
<th>section</th>
<th>v2.2.0-2</th>
<th>v2.2.1-1</th>
<th>v2.2.1-2</th>
<th>v2.2.1-3</th>
<th>v2.2.2-1</th>
<th>v2.2.2-2</th>
<th>v2.2.3-1</th>
<th>v2.2.3-2</th>
<th>v2.2.5-1</th>
<th>v2.2.5-2</th>
<th>v2.2.5-3</th>
<th>v2.2.6-1</th>
<th>v2.2.6-2</th>
<th>...+deb10u1</th>
<th>...+deb10u2</th>
<th>...+deb10u3</th>
<th>...+deb10u4</th>
<th>...+deb10u5</th>
<th>...+deb10u6</th>
</tr>
</thead>
<tbody>
<tr>
<td>.note</td>
<td>-</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>.init</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>.text</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>.rodata</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>.relro</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>.data</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>.bss</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>updatable</td>
<td>-</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>-</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

- ○: compatible change
- ●: incompatible change
## LUCI Compatibility Analysis

### EXPAT from Debian Buster

<table>
<thead>
<tr>
<th>section</th>
<th>v2.2.0-2</th>
<th>v2.2.1-1</th>
<th>v2.2.1-2</th>
<th>v2.2.1-3</th>
<th>v2.2.2-1</th>
<th>v2.2.2-2</th>
<th>v2.2.3-1</th>
<th>v2.2.3-2</th>
<th>v2.2.4-1</th>
<th>v2.2.5-1</th>
<th>v2.2.5-2</th>
<th>v2.2.5-3</th>
<th>v2.2.6-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>.note</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>.init</td>
<td>-</td>
<td>-</td>
<td>○</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>.text</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>.rodata</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>.relro</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>.data</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>.bss</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

**Development**

| updatable | - | ✓ | ✓ | ✓ | - | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

**Stable**

| updatable | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

○ compatible change  ● incompatible change
Test Application

EXPAT from Debian Buster

Testcases:
- Successful
- Failed
- Skipped

Heinloth et al.

LUCI
Test Application with LUCI Dynamic Updates

EXPAT from Debian Buster

Testcases

- Restart
- Successful
- Failed
- Skipped

Heinloth et al.
## Summary

<table>
<thead>
<tr>
<th>Build</th>
<th>Expat</th>
<th>dynamic updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>custom (vanilla)</td>
<td>2.0.0 – 2.5.0</td>
<td>17 / 26 (65%)</td>
</tr>
<tr>
<td>Debian Buster</td>
<td>all 2.2.0 – 2.2.6</td>
<td>13 / 18 (72%)</td>
</tr>
<tr>
<td></td>
<td>stable 2.2.6</td>
<td>6 / 6 (100%)</td>
</tr>
<tr>
<td>Debian Bullseye</td>
<td>all 2.2.7 – 2.2.10</td>
<td>9 / 10 (90%)</td>
</tr>
<tr>
<td></td>
<td>stable 2.2.10</td>
<td>5 / 5 (100%)</td>
</tr>
<tr>
<td>Ubuntu Focal</td>
<td>all 2.2.7 – 2.2.9</td>
<td>6 / 6 (100%)</td>
</tr>
<tr>
<td></td>
<td>stable 2.2.9</td>
<td>4 / 4 (100%)</td>
</tr>
<tr>
<td>Ubuntu Jammy</td>
<td>all 2.4.1 – 2.4.7</td>
<td>10 / 12 (83%)</td>
</tr>
<tr>
<td></td>
<td>stable 2.4.7</td>
<td>2 / 2 (100%)</td>
</tr>
</tbody>
</table>
Luci applying majority of releases without restart

- ✓ Expat XML Parser
- ✓ Libxcrypt (Extended Crypt Library)
- ✗ OpenSSL
- ✓ PECL (Perl 5 Compatible Regular Expression Library)
- ✓ Zlib
Conclusion
Dynamic linker/loader (RTLD) with DSU-capabilities for libraries

- ready for off-the-shelf shared objects by adapting techniques for dynamic linking
- conforming to today’s package distribution
- transparent to the user
- no runtime overhead
- sufficient for common bugfix changes

*Source and Artifact available at github.com/luci-project/eval-atc23*
Thank you!