Mayhem for Code

T nathan / tutorial › lighttpd › Run 1

Defects

Overview

8 defects found in this run.

Target Defect ID	Seen in Task	Example Test Case	Time First Seen
TDID-1386: Out-of-bounds Read	Behavior Testing	ba0dbafbd0b787a564635b887f77926ae0b3f979dcc7 2d30cf7fdb1707581919	00:36
TDID-1385: Out-of-bounds Write	Behavior Testing	ba0dbafbd0b787a564635b887f77926ae0b3f979dcc7 2d30cf7fdb1707581919	00:36
TDID-1384: Out-of-bounds Read	Behavior Testing	ba0dbafbd0b787a564635b887f77926ae0b3f979dcc7 2d30cf7fdb1707581919	00:36
TDID-1383: Out-of-bounds Read	Behavior Testing	ba0dbafbd0b787a564635b887f77926ae0b3f979dcc7 2d30cf7fdb1707581919	00:36
TDID-1382: Out-of-bounds Read	Behavior Testing	ba0dbafbd0b787a564635b887f77926ae0b3f979dcc7 2d30cf7fdb1707581919	00:36
TDID-1381: Out-of-bounds Read	Behavior Testing	ba0dbafbd0b787a564635b887f77926ae0b3f979dcc7 2d30cf7fdb1707581919	00:36
TDID-1380: Out-of-bounds Read	Behavior Testing	ba0dbafbd0b787a564635b887f77926ae0b3f979dcc7 2d30cf7fdb1707581919	00:36
TDID-1379: Improper Input Validation	Behavior Testing	ba0dbafbd0b787a564635b887f77926ae0b3f979dcc7 2d30cf7fdb1707581919	00:36

Defect Details

TDID-1386: Out-of-bounds Read (CWE-125)

The software reads data past the end, or before the beginning, of the intended buffer.

Runtime Errors

Error	Severity	Description
1. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c18f in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:177
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

2. Invalid Write	High	Invalid write of size 1

Error	Severity	Description

Backtrace

```
0x483c864 in memmove() /workdir/build/valgrind-3.16.1/memcheck/../shared/vg_replace_strmem.c:1270
0x11c18e in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:176
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

3. Invalid Read — Medium — Invalid read of size 8

Backtrace

```
0x11c181 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:176
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

4. Invalid Read — Medium — Invalid read of size 8

Backtrace

```
0x11c174 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:173
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

5. Invalid Read — Medium — Invalid read of size 8

Backtrace

```
0x11bf16 in buffer_prepare_append() /build/lighttpd-1.4.15/src/buffer.c:111
0x11c173 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:172
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

6. Invalid Read — Medium — Invalid read of size 8

Backtrace

```
0x11bf0a in buffer_prepare_append() /build/lighttpd-1.4.15/src/buffer.c:102
0x11c173 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:172
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

7. Invalid Read — Medium — Invalid read of size 8

TDID-1385: Out-of-bounds Write (CWE-787)

The software writes data past the end, or before the beginning, of the intended buffer.

Runtime Errors

Error	Severity	Description
1. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c18f in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:177
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

2. Invalid Write	High	Invalid write of size 1

Backtrace

```
0x483c864 in memmove() /workdir/build/valgrind-3.16.1/memcheck/../shared/vg_replace_strmem.c:1270
0x11c18e in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:176
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

3. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c181 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:176
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

4. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c174 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:173
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

5. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11bf16 in buffer_prepare_append() /build/lighttpd-1.4.15/src/buffer.c:111
0x11c173 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:172
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

Error	Severity	Description
6. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11bf0a in buffer_prepare_append() /build/lighttpd-1.4.15/src/buffer.c:102
0x11c173 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:172
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

Error	Severity	Description
7. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11a72c in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

TDID-1384: Out-of-bounds Read (CWE-125)

The software reads data past the end, or before the beginning, of the intended buffer.

Runtime Errors

Error	Severity	Description
1. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c18f in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:177
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

2. Invalid Write	High	Invalid write of size 1

Backtrace

```
0x483c864 in memmove() /workdir/build/valgrind-3.16.1/memcheck/../shared/vg_replace_strmem.c:1270
0x11c18e in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:176
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

3. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c181 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:176
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

4. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c174 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:173
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

5. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11bf16 in buffer_prepare_append() /build/lighttpd-1.4.15/src/buffer.c:111
0x11c173 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:172
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

Error	Severity	Description
6. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11bf0a in buffer_prepare_append() /build/lighttpd-1.4.15/src/buffer.c:102
0x11c173 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:172
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

7. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11a72c in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

TDID-1383: Out-of-bounds Read (CWE-125)

The software reads data past the end, or before the beginning, of the intended buffer.

Runtime Errors

Error	Severity	Description
1. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c18f in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:177
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

2. Invalid Write	High	Invalid write of size 1

Backtrace

```
0x483c864 in memmove() /workdir/build/valgrind-3.16.1/memcheck/../shared/vg_replace_strmem.c:1270
0x11c18e in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:176
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

3. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c181 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:176
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

4. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c174 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:173
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

5. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11bf16 in buffer_prepare_append() /build/lighttpd-1.4.15/src/buffer.c:111
0x11c173 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:172
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

Error	Severity	Description
6. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11bf0a in buffer_prepare_append() /build/lighttpd-1.4.15/src/buffer.c:102
0x11c173 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:172
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

Error	Severity	Description
7. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11a72c in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

TDID-1382: Out-of-bounds Read (CWE-125)

The software reads data past the end, or before the beginning, of the intended buffer.

Runtime Errors

Error	Severity	Description
1. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c18f in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:177
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

2. Invalid Write	High	Invalid write of size 1

Backtrace

```
0x483c864 in memmove() /workdir/build/valgrind-3.16.1/memcheck/../shared/vg_replace_strmem.c:1270
0x11c18e in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:176
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

3. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c181 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:176
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

4. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c174 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:173
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

5. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11bf16 in buffer_prepare_append() /build/lighttpd-1.4.15/src/buffer.c:111
0x11c173 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:172
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

Error	Severity	Description
6. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11bf0a in buffer_prepare_append() /build/lighttpd-1.4.15/src/buffer.c:102
0x11c173 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:172
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

Error	Severity	Description
7. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11a72c in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

TDID-1381: Out-of-bounds Read (CWE-125)

The software reads data past the end, or before the beginning, of the intended buffer.

Runtime Errors

Error	Severity	Description
1. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c18f in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:177
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

2. Invalid Write	High	Invalid write of size 1

Backtrace

```
0x483c864 in memmove() /workdir/build/valgrind-3.16.1/memcheck/../shared/vg_replace_strmem.c:1270
0x11c18e in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:176
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

3. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c181 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:176
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

4. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c174 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:173
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

5. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11bf16 in buffer_prepare_append() /build/lighttpd-1.4.15/src/buffer.c:111
0x11c173 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:172
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

Error	Severity	Description
6. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11bf0a in buffer_prepare_append() /build/lighttpd-1.4.15/src/buffer.c:102
0x11c173 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:172
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

Error	Severity	Description
7. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11a72c in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

TDID-1380: Out-of-bounds Read (CWE-125)

The software reads data past the end, or before the beginning, of the intended buffer.

Runtime Errors

Error	Severity	Description
1. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c18f in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:177
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

2. Invalid Write	High	Invalid write of size 1

Backtrace

```
0x483c864 in memmove() /workdir/build/valgrind-3.16.1/memcheck/../shared/vg_replace_strmem.c:1270
0x11c18e in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:176
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

3. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c181 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:176
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

4. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11c174 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:173
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

5. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11bf16 in buffer_prepare_append() /build/lighttpd-1.4.15/src/buffer.c:111
0x11c173 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:172
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

Error	Severity	Description
6. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11bf0a in buffer_prepare_append() /build/lighttpd-1.4.15/src/buffer.c:102
0x11c173 in buffer_append_string() /build/lighttpd-1.4.15/src/buffer.c:172
0x11a737 in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

Error	Severity	Description
7. Invalid Read	Medium	Invalid read of size 8

Backtrace

```
0x11a72c in http_request_parse() /build/lighttpd-1.4.15/src/request.c:740
0x114478 in connection_state_machine() /build/lighttpd-1.4.15/src/connections.c:1374
0x115012 in network_server_handle_fdevent() /build/lighttpd-1.4.15/src/network.c:51
0x11048d in main() /build/lighttpd-1.4.15/src/server.c:1309
```

TDID-1379: Improper Input Validation (CWE-20)

The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.

Test Case

```
ba0dbafbd0b787a564635b887f77926ae0b3f979dcc72d30cf7fdb1707581919
```

Output

```
Standard Out: (empty)

Standard Error:
2022-02-14 17:28:04: (log.c.75) server started
```

Backtrace

```
#0 0x7ffff7e3e7bb in __GI_raise at /build/glibc-vjB4T1/glibc-2.28/signal/../sysdeps/unix/sysv/linux/raise.c:51:1
#1 0x7ffff7e29535 in __GI_abort at /build/glibc-vjB4T1/glibc-2.28/stdlib/abort.c:81:7
#2 0x7ffff7e80508 in __printf_fphex at /build/glibc-vjB4T1/glibc-2.28/stdio-common/../stdio-common/printf_fphex.c:233:2
#3 0x7ffff7e86c1a in _IO_vfwprintf at /build/glibc-vjB4T1/glibc-2.28/stdio-common/vfprintf.c:1638:4
#4 0x7ffff7e886fd in _IO_vfscanf_internal at /build/glibc-vjB4T1/glibc-2.28/stdio-common/vfscanf.c:1890:8
#5 0x7ffff7e8ad80 in _IO_vfscanf_internal at /build/glibc-vjB4T1/glibc-2.28/stdio-common/vfscanf.c:1834:5
#6 0x7ffff7e8bd4f in _IO_vfscanf_internal at /build/glibc-vjB4T1/glibc-2.28/stdio-common/vfscanf.c:2922:18
#7 0x555555567f47 in connection_state_machine at /build/lighttpd-1.4.15/src/connections.c:1709:3
#8 0x555555568174 in network_server_init at /build/lighttpd-1.4.15/src/network.c:155:5
#9 0x555555566738 in connection_handle_read at /build/lighttpd-1.4.15/src/connections.c:311:5 (inlined by)
connection_handle_read_state at /build/lighttpd-1.4.15/src/connections.c:861:10
#10 0x555555560479 in connection_state_machine at /build/lighttpd-1.4.15/src/connections.c:1374:7
#11 0x555555561013 in network_server_handle_fdevent at /build/lighttpd-1.4.15/src/network.c:53:14
#12 0x55555555c48e in main at /build/lighttpd-1.4.15/src/server.c:1309:18
#13 0x7ffff7e2b09b in __libc_start_main at /build/glibc-vjB4T1/glibc-2.28/csu/../csu/libc-start.c:342:3
#14 0x55555555d2da in _start+0x2a at ??:0:0
```

Disassembly

```
0x7ffff7e3e7bb: mov     rcx, qword ptr [rsp + 0x108]
0x7ffff7e3e7c3: xor     rcx, qword ptr fs:[0x28]
0x7ffff7e3e7cc: mov     eax, r8d
0x7ffff7e3e7cf: jne     0x7ffff7e3e7ee
0x7ffff7e3e7d1: add     rsp, 0x110
0x7ffff7e3e7d8: pop     rbx
0x7ffff7e3e7d9: ret
0x7ffff7e3e7da: nop     word ptr [rax + rax]
0x7ffff7e3e7e0: mov     rdx, qword ptr [rip + 0x183689]
0x7ffff7e3e7e7: neg     eax
0x7ffff7e3e7e9: mov     dword ptr fs:[rdx], eax
0x7ffff7e3e7ec: jmp     0x7ffff7e3e7a4
0x7ffff7e3e7ee: call    0x7ffff7f117b0
0x7ffff7e3e7f3: nop     word ptr cs:[rax + rax]
0x7ffff7e3e7fd: nop     dword ptr [rax]
0x7ffff7e3e800: test    edi, edi
0x7ffff7e3e802: js      0x7ffff7e3e810
0x7ffff7e3e804: neg     edi
0x7ffff7e3e806: jmp     0x7ffff7e3ea90
0x7ffff7e3e80b: nop     dword ptr [rax + rax]
0x7ffff7e3e810: mov     rax, qword ptr [rip + 0x183659]
0x7ffff7e3e817: mov     dword ptr fs:[rax], 0x16
```

Register State

```
rax 0x0
rbx 0x6
rcx 0x7ffff7e3e7bb
rdx 0x0
rsi 0x7fffffffdfb0
rdi 0x2
rbp 0x7fffffffe300
rsp 0x7fffffffdfb0
r8 0x0
r9 0x7fffffffdfb0
r10 0x8
r11 0x246
r12 0x7fffffffe220
r13 0x1000
r14 0x10
```

```
r15 0x7ffff7fd0000
rip 0x7ffff7e3e7bb
```

Signal Number

```
6
```

Memory Maps

```
555555554000-55555555b000 r--p 00000000 08:01 2092863                    /usr/local/sbin/lighttpd
55555555b000-555555574000 r-xp 00007000 08:01 2092863                    /usr/local/sbin/lighttpd
555555574000-55555557f000 r--p 00020000 08:01 2092863                    /usr/local/sbin/lighttpd
55555557f000-555555580000 r--p 0002a000 08:01 2092863                    /usr/local/sbin/lighttpd
555555580000-555555581000 rw-p 0002b000 08:01 2092863                    /usr/local/sbin/lighttpd
555555581000-5555555e4000 rw-p 00000000 00:00 0                          [heap]
7ffff7dec000-7ffff7ded000 r--p 00000000 08:01 2092852                    /usr/local/lib/mod_staticfile.so
7ffff7ded000-7ffff7def000 r-xp 00001000 08:01 2092852                    /usr/local/lib/mod_staticfile.so
7ffff7def000-7ffff7df0000 r--p 00003000 08:01 2092852                    /usr/local/lib/mod_staticfile.so
7ffff7df0000-7ffff7df1000 r--p 00003000 08:01 2092852                    /usr/local/lib/mod_staticfile.so
7ffff7df1000-7ffff7df2000 rw-p 00004000 08:01 2092852                    /usr/local/lib/mod_staticfile.so
7ffff7df2000-7ffff7df4000 r--p 00000000 08:01 2092814                    /usr/local/lib/mod_dirlisting.so
7ffff7df4000-7ffff7df6000 r-xp 00002000 08:01 2092814                    /usr/local/lib/mod_dirlisting.so
7ffff7df6000-7ffff7df7000 r--p 00004000 08:01 2092814                    /usr/local/lib/mod_dirlisting.so
7ffff7df7000-7ffff7df8000 r--p 00004000 08:01 2092814                    /usr/local/lib/mod_dirlisting.so
7ffff7df8000-7ffff7df9000 rw-p 00005000 08:01 2092814                    /usr/local/lib/mod_dirlisting.so
7ffff7df9000-7ffff7dfa000 r--p 00000000 08:01 2092802                    /usr/local/lib/mod_accesslog.so
7ffff7dfa000-7ffff7dfc000 r-xp 00001000 08:01 2092802                    /usr/local/lib/mod_accesslog.so
7ffff7dfc000-7ffff7dfd000 r--p 00003000 08:01 2092802                    /usr/local/lib/mod_accesslog.so
7ffff7dfd000-7ffff7dfe000 r--p 00003000 08:01 2092802                    /usr/local/lib/mod_accesslog.so
7ffff7dfe000-7ffff7dff000 rw-p 00004000 08:01 2092802                    /usr/local/lib/mod_accesslog.so
7ffff7dff000-7ffff7e00000 r--p 00000000 08:01 2092828                    /usr/local/lib/mod_indexfile.so
7ffff7e00000-7ffff7e01000 r-xp 00001000 08:01 2092828                    /usr/local/lib/mod_indexfile.so
7ffff7e01000-7ffff7e02000 r--p 00002000 08:01 2092828                    /usr/local/lib/mod_indexfile.so
7ffff7e02000-7ffff7e03000 r--p 00002000 08:01 2092828                    /usr/local/lib/mod_indexfile.so
7ffff7e03000-7ffff7e04000 rw-p 00003000 08:01 2092828                    /usr/local/lib/mod_indexfile.so
7ffff7e04000-7ffff7e07000 rw-p 00000000 00:00 0
7ffff7e07000-7ffff7e29000 r--p 00000000 08:01 1961998                    /lib/x86_64-linux-gnu/libc-2.28.so
7ffff7e29000-7ffff7f71000 r-xp 00022000 08:01 1961998                    /lib/x86_64-linux-gnu/libc-2.28.so
7ffff7f71000-7ffff7fbd000 r--p 0016a000 08:01 1961998                    /lib/x86_64-linux-gnu/libc-2.28.so
7ffff7fbd000-7ffff7fbe000 ---p 001b6000 08:01 1961998                    /lib/x86_64-linux-gnu/libc-2.28.so
7ffff7fbe000-7ffff7fc2000 r--p 001b6000 08:01 1961998                    /lib/x86_64-linux-gnu/libc-2.28.so
7ffff7fc2000-7ffff7fc4000 rw-p 001ba000 08:01 1961998                    /lib/x86_64-linux-gnu/libc-2.28.so
7ffff7fc4000-7ffff7fc8000 rw-p 00000000 00:00 0
7ffff7fc8000-7ffff7fc9000 r--p 00000000 08:01 1961666                    /lib/x86_64-linux-gnu/libdl-2.28.so
7ffff7fc9000-7ffff7fca000 r-xp 00001000 08:01 1961666                    /lib/x86_64-linux-gnu/libdl-2.28.so
7ffff7fca000-7ffff7fcb000 r--p 00002000 08:01 1961666                    /lib/x86_64-linux-gnu/libdl-2.28.so
7ffff7fcb000-7ffff7fcc000 r--p 00002000 08:01 1961666                    /lib/x86_64-linux-gnu/libdl-2.28.so
7ffff7fcc000-7ffff7fcd000 rw-p 00003000 08:01 1961666                    /lib/x86_64-linux-gnu/libdl-2.28.so
7ffff7fcd000-7ffff7fcf000 rw-p 00000000 00:00 0
7ffff7fd0000-7ffff7fd1000 rw-p 00000000 00:00 0
7ffff7fd1000-7ffff7fd4000 r--p 00000000 00:00 0                          [vvar]
7ffff7fd4000-7ffff7fd5000 r-xp 00000000 00:00 0                          [vdso]
7ffff7fd5000-7ffff7fd6000 r--p 00000000 08:01 1961984                    /lib/x86_64-linux-gnu/ld-2.28.so
7ffff7fd6000-7ffff7ff4000 r-xp 00001000 08:01 1961984                    /lib/x86_64-linux-gnu/ld-2.28.so
7ffff7ff4000-7ffff7ffc000 r--p 0001f000 08:01 1961984                    /lib/x86_64-linux-gnu/ld-2.28.so
7ffff7ffc000-7ffff7ffd000 r--p 00026000 08:01 1961984                    /lib/x86_64-linux-gnu/ld-2.28.so
7ffff7ffd000-7ffff7ffe000 rw-p 00027000 08:01 1961984                    /lib/x86_64-linux-gnu/ld-2.28.so
7ffff7ffe000-7ffff7fff000 rw-p 00000000 00:00 0
7ffffffde000-7ffffffff000 rw-p 00000000 00:00 0                          [stack]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0                  [vsyscall]
```