w3m Certificate Handling Format String Vulnerability

2006-12-26 17:19:07 by Raven

SECUNIA ADVISORY ID: SA23492

VERIFY ADVISORY: http://secunia.com/advisories/23492/

CRITICAL: Highly critical

IMPACT: System access

SOFTWARE: w3m 0.x - http://secunia.com/product/12960/

DESCRIPTION: A vulnerability has been reported in w3m, which potentially can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a format string error when handling SSL certificates and can be exploited via a specially crafted SSL certificate containing format specifiers in the "CN" field. Successful exploitation may allow execution of arbitrary code when e.g. visiting a malicious website, but requires that the application is running with either the "-dump" or "-backend" option. The vulnerability is reported in version 0.5.1. Other versions may also be affected.

SOLUTION: Only visit trusted sites when running with the "-backend" or "-dump" options.

PROVIDED AND/OR DISCOVERED BY: Reported by an anonymous person.

ORIGINAL ADVISORY: http://sourceforge.net/tracker/index.php?func=detail&aid=1612792&group_id=39518&atid=425439