

HIO-BUG-092408 Autopsy Forensic Browser Script Insertion

The Autopsy Forensic Browser contains a flaw which could be exploited to conduct script insertions, but do so would be very difficult given additional application security methods.

The Autopsy Forensic Browser is a graphical interface to the command line digital investigation analysis tools in The Sleuth Kit. Together, they can analyze Windows and UNIX disks and file systems (NTFS, FAT, UFS1/2, Ext2/3).

This flaw exists because the application does not validate the "host" variable upon submission to the autopsy.pl script. This can be exploited to insert arbitrary HTML and script code, which will be executed in a user's browser session in context of an affected Autopsy instance.

Status: Very difficult to exploit.

From CHANGES.txt: Bug Fix: Input check on host was printing invalid host values w/out encoding HTML entities.

References: Vendor Solution: Upgrade to version 2.20