

IT security: Vulnerabilities in Google Chrome

The US Government's Cyber Security Bulletin released late last night includes notifications of security vulnerabilities in previous builds of Google Chrome.

Google Chrome is underpinned by Apple's Safari and includes some of the latter's quirks especially in handling certain Javascript controls.

However, there are no similar warnings relating to Safari.

The "high vulnerability" warnings related to Google Chrome are:

Google Chrome before 5.0.375.55 does not properly execute JavaScript code in the extension context, which has unspecified impact and remote attack vectors.

Unspecified vulnerability in Google Chrome before 5.0.375.55 allows user-assisted remote attackers to cause a denial of service (memory error) or possibly have unspecified other impact via vectors related to the "drag + drop" functionality.

Unspecified vulnerability in Google Chrome before 5.0.375.55 allows remote attackers to bypass the whitelist-mode plugin blocker via unknown vectors.

Unspecified vulnerability in Google Chrome before 5.0.375.55 allows attackers to cause a denial of service (memory error) or possibly have unspecified other impact via vectors related to the Safe Browsing functionality.

Unspecified vulnerability in Google Chrome before 5.0.375.55 might allow remote attackers to spoof the URL bar via vectors involving unload event handlers.

Google Chrome before 5.0.375.55 does not properly follow the Safe Browsing specification's requirements for canonicalization of URLs, which has unspecified impact and remote attack vectors.

Medium Vulnerability

Google Chrome 1.0.154.48 allows remote attackers to cause a denial of service (resource consumption) via JavaScript code containing an infinite loop that creates IFRAME elements for invalid news:// URIs.

Vulnerabilities (Medium or low) were also reported for Microsoft Internet Explorer and Firefox (the core of which is used by several other browsers but which were not mentioned)

The reports are dated, in some cases, up to 9 days ago and the recommended fix is, as always, to make sure that the latest version of the program is installed.

Apple announced the release of Safari 5.0 yesterday.