# CVE Detail – CVE-2010-4577

The CSSParser::parseFontFaceSrc function in WebCore/css/CSSParser.cpp in WebKit, as used in Google Chrome before 8.0.552.224, Chrome OS before 8.0.552.343, webkitgtk before 1.2.6, and other products does not properly parse Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted local font, related to "Type Confusion."

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.88341

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-125: Out-of-bounds Read
* CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')

## CAPEC(s)

* CAPEC-540: Overread Buffers

## Affected Products

* cpe:2.3:a:google:chrome:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:webkitgtk:webkitgtk:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:google:chrome\_os:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:13:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:7.0:\*:\*:\*:\*:\*:\*:\*