

Common Vulnerability Research

NSS-1404_Week4

Jeramie Brehm

Buffer Overflow: Adobe Flash Player < 11.2.202.350

NIST ID: CVE-2014-0515

Impact: Unauthorized information disclosure, modification, and disruption of service.

Synopsis: Player susceptible to buffer-overflow vulnerability due to improperly checking user-supplied data before copying the data into an insufficient sized buffer. Exploit condition executes arbitrary code within the application. Possibility of denial of service condition present on failed exploit attempts.

Affected Area: Linux version of Adobe Flash Player 11.2.202.350 and earlier.

Known Fix: Update to Adobe Flash Player 11.2.202.356 for Linux.