



Date: 19/06/2008

---

## Mozilla Firefox Zero Day Vulnerability - Advisory

---

GovCertUK have been made aware of a 0-day Critical vulnerability affecting both the newly released Firefox 3.0 browser, along with older 2.0.x releases. Successful exploitation of the vulnerability could allow an attacker to execute arbitrary code on the client machine.

### Affected Software

Mozilla Firefox 3.0  
Mozilla Firefox 2.0.x (all versions)

### Vulnerability Details

Firefox 3.0 was released by Mozilla on 18/06/08, and approximately five hours later a submission was made to the Zero Day initiative detailing the 0-day vulnerability in the browser. They have verified the vulnerability and reported it privately to Mozilla.

To successfully exploit this vulnerability user interaction is required, typically visiting a malicious website or clicking a link in an email.

There is currently no patch available.

### Comment / Mitigation

- There are currently no known exploits for this vulnerability
- Until Mozilla release a fix, users should consider using an alternative browser.
- Mitigation set 1 applies.

## Firefox 0-day Advisory – 19<sup>th</sup> June 2008

---

### Mitigation Information and factors

Mitigation refers to a software setting, common configuration or general best practice, existing in a default state that could reduce the severity of exploitation of vulnerability. The following mitigating factors may be helpful for securing your systems.

#### Mitigation factors – Set 1

- In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content could contain specially crafted content that could exploit this vulnerability. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail or Instant Messenger message that takes users to the attacker's Web site.
- An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

### References

<http://dvlabs.tippingoint.com/blog/2008/06/18/vulnerability-in-mozilla-firefox-30>

Telephone:	01242 709311
Fax:	01242 709113
General Enquiries:	<a href="mailto:enquiries@govcertuk.gov.uk">enquiries@govcertuk.gov.uk</a>
Incidents & Alerts:	<a href="mailto:incidents@govcertuk.gov.uk">incidents@govcertuk.gov.uk</a>
Restricted Communications (GSI only):	<a href="mailto:govcertuk@cesg.gsi.gov.uk">govcertuk@cesg.gsi.gov.uk</a>
Website:	<a href="http://www.govcertuk.gov.uk">www.govcertuk.gov.uk</a>