

## FAST DNS analysis vulnerability

<b>Date discovered</b>	29 May 2006
<b>Bulletin issued</b>	AK-2006-02 1.0 (06 June 2006)
<b>Importance</b>	High
<b>Impact</b>	Denial of service
<b>Level of competence required to launch an attack</b>	Medium
<b>Source of the attack</b>	Internet
<b>How widely available?</b>	Medium
<b>Arkoon versions</b>	All

### Introduction

A vulnerability which would allow an attacker to reboot a FAST360 appliance has been uncovered in the FAST DNS module. A reboot can be triggered by a malformed DNS message.

This vulnerability was detected using a suite of tests developed by the University of Oulu (details at <http://www.ee.oulu.fi/research/ouspg/protos/testing/c09/dns/index.html>).

All FAST360 UTM appliances running versions 3.0, 3.1, 3.2, 3.3 and 4.0 and using the FAST DNS module are vulnerable.

Note: this vulnerability can only be exploited under certain specific conditions. In particular, it is difficult to carry out from the Internet unless the FAST360 appliance is positioned to protect a public DNS server.

See the section '*Identifying Vulnerable Configurations*' below to find out if your appliances are impacted.

### Description

#### Impact

This vulnerability allows an attacker to trigger a reboot of the FAST360 appliance, effectively a denial of service attack as communications are interrupted.

The FAST360 appliance needs to be configured to permit DNS traffic (flow rules). The vulnerability does not allow arbitrary code to be executed on the appliance.



## Risk

This vulnerability is classified as HIGH RISK for the following reasons:

- Attack possible from the Internet (depending on device configuration)
- Successful attacks result in denial of service.

## Identifying Vulnerable Configurations

### Impacted versions:

- Major release 3.0 <= 3.0/29
- Intermediate releases 3.x: all 3.1, 3.2, 3.3 versions (no longer supported)
- Major release 4.0 (4.0/1)

### Impacted configurations:

- Any configuration in which the FAST DNS module is activated

Note: The FAST DNS module is activated by default in the implicit rules generated when DNS server access is configured on a FAST360 appliance.

## Solution

This problem is fixed in versions 3.0/30 and 4.0/2. If you have a vulnerable configuration, we recommend that you update as soon as possible.

Note: With the release of version 4.0/1, Arkoon FAST360 versions 3.1, 3.2 et 3.3 are no longer supported. If you are running an unsupported release we recommend that you upgrade to version 4.0/2 as soon as possible.

If you have any problems, contact the Arkoon support team by visiting <http://client.arkoon.net>

Best regards

Arkoon Security Team  
[security@arkoon.net](mailto:security@arkoon.net)

