

Possibility of by-passing FAST HTTP and IDPS HTTP analysis

Date discovered	31 March 2006
Bulletin issued	AK-2006-01 1.0 (6 June 2006)
Importance	High
Impact	By-passing of security policies
Level of competence required to launch an attack	Medium
Source of the attack	Internet
How widely available?	Not public
Arkoon versions	All FAST360 3.x versions

Introduction

A vulnerability allowing an attacker to by-pass FAST and IDPS analysis of HTTP traffic has been identified in certain FAST360 releases. An attack using this method can by-pass the FAST and IDPS HTTP filtering mechanisms, in particular IDPS keyword filtering.

All FAST360 UTM appliances running versions 3.0, 3.1, 3.2 or 3.3 with FAST HTTP and/or IDPS HTTP analysis enabled are vulnerable. The vulnerability is not present in version 4.0.

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

Description

The vulnerability is located in code handling URL analysis in the FAST HTTP and IDPS http components. In certain cases URLs may be misinterpreted, preventing correct keyword and signature analysis and filtering by the IDPS module.

Impact

This vulnerability could be used to by-pass configured security policies, in particular:

- By-passing keyword filtering in the FAST http module;
- By-passing signature-based attack detection by the IDPS http module (in HTTP_URL state).



Risk

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

- attacks can be launched from the Internet;
- IDPS HTTP signatures can be by-passed;
- Configured security policies can be by-passed.

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)

Impacted configurations:

- Any configuration in which the FAST HTTP module is activated (with or without IDPS HTTP)

Note : The FAST HTTP module is activated by default when the HTTP proxy is enabled.

Solution

This problem is fixed in versions 3.0/30 and 4.0/1. 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 4.0/1 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

