Threat Category: Web Application Attack, IIS Vulnerability

Threat Description: The rule is designed to detect attempts to access the trace.axd file on Microsoft IIS web servers. This file is a debugging tool that, if accessible, can expose sensitive information. This rule focuses on traffic from an external network to internal HTTP servers. The detection mechanism involves checking the HTTP URI for the presence of the string "/trace.axd". The rule uses http_uri, fast_pattern, and nocase keywords.

Indicators of Compromise (IoCs):

HTTP URI: "/trace.axd"

Detection Mechanism:

The network protocol must be TCP.

The traffic direction must be from $EXTERNAL_NET to $HTTP_SERVERS on $HTTP_PORTS.

The TCP connection must be established (established).

The HTTP URI must contain the string "/trace.axd".

The rule uses fast_pattern for efficient matching and nocase for case-insensitive matching.

Possible Attribution & Use Cases: The detection can be used to identify attempts to access sensitive information via the trace.axd file on IIS servers.

This rule is useful for monitoring web traffic for potentially malicious activity targeting web servers.

Recommended Actions:

Monitor and Investigate: If this rule is triggered, investigate the source of the traffic and the targeted web server to determine if the trace.axd file is exposed.

Remove or Restrict Access: Remove the trace.axd file or restrict access to it to prevent unauthorized access to sensitive information.

Author & Attribution:

Rule Author: Community

Rule Source: Community

Rule SID: 1660

Rule Revision: 19

Service: http

Metadata: policy max-detect-ips drop

Reference: Nessus-10993