Threat Category: Web Application Attack, Microsoft FrontPage Vulnerability

Threat Description: The rule is designed to detect attempts to access Microsoft FrontPage's /_vti_bin/ directory. This directory is associated with FrontPage Server Extensions, which have been known to contain vulnerabilities. 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 "/_vti_bin/". The rule uses http_uri, fast_pattern, and nocase keywords.

Indicators of Compromise (IoCs):

HTTP URI: "/_vti_bin/"

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 "/_vti_bin/".

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 exploit vulnerabilities in Microsoft FrontPage Server Extensions.

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 for potential exploitation.

Disable FrontPage Extensions: If possible, disable FrontPage Server Extensions as they are often unnecessary and pose a security risk.

Author & Attribution:

Rule Author: Community

Rule Source: Community

Rule SID: 1288

Rule Revision: 18

Service: http

Metadata: policy max-detect-ips drop

Reference: Nessus-11032