Intrusion Prevention | FortiGuard Labs

Archived: 2026-04-05 21:09:46 UTC

Description

This indicates an attempt to access ReGeorg HTTP Tunnel.
ReGeorg acts as a HTTP proxy to tunnel data in and out of a network. It is used to bypass firewall policy that only allows HTTP traffics. ReGeorg can transport other TCP sessions such as RDP, SSH, and SMB through the HTTP tunnel.
ReGeorg is an upgraded version of ReDuh. The ReGeorg server script is often installed by attackers after a web server is compromised.

Affected Products

All web servers

Impact

System Compromise: Remote attackers can gain control of vulnerable systems.

Recommended Actions

Monitor the traffic from the network for any suspicious activity.
Look for a suspicious PHP, ASP, JSP, or JS file on the web server, based on the IPS log entry.

Last 24 Hours

0

Daily Trend

0%

Last 7 Days

0

Weekly Trend

0%

Coverage

IPS (Regular DB)	
IPS (Extended DB)	

Version Updates

Date	Version	Status	Detail
2019-04-05	14.587		Default_action:pass:drop
2019-03-13	14.572		Sig Added
2019-03-12	14.571		
