Release Notes for URL Category and Threat Category Updates for Cisco Web and Email Security Appliances

Contents

URL Category Updates

Release Date

Release Date: February 8, 2021

Changes

Two existing URL categories removed:

- Health and Nutrition
- Nature

For more information on the changes made to Cisco Talos's URL Category lists, see the Cisco Talos blog at https://blog.talosintelligence.com/2021/01/2021-changes-to-content-and-threat-categories.html.

Release Date

Release Date: January 21, 2021

Changes

Fifteen new URL categories added:

- **Cannabis** - Websites that focus on the recreational and medicinal consumption of cannabis.

- **Cloud and Data Centers** - Platforms used to serve cloud infrastructure or data center hosting to support an organization's applications, services, or data processing.

- **Conventions, Conferences and Trade Shows** - Seminars, trade shows, conventions and conferences themed around a particular industry, market, or common interest.

- **Cryptocurrency** - Online brokerages and websites that enable users to trade cryptocurrencies; information regarding cryptocurrencies including analysis, commentary, advice, performance indexes, and price charts.

- **Cryptomining** - Hosts that are actively participating in a cryptocurrency mining pool.

- **DoH and DoT** -Encrypted DNS requests using either the DNS over HTTPS (DoH) protocol or the DNS over TLS (DoT) protocol.

- **DNS-Tunneling** - Sites that provide DNS-Tunneling as a service. These services can be for PC or mobile and create a VPN connection specifically over DNS to send traffic that may bypass corporate policies and inspection.

- **Dynamic DNS Provider** - Users may use dynamic DNS services to make certain applications or content accessible via the web from endpoints hosted on dynamically assigned IP addresses.

- **Internet of Things** - Domains used to monitor the general health, activity, or aid in the configuration of Internet of Things (IoT) and other network-aware electronics.

- **Museums** - Museums and exhibits, both online and physical, dedicated to preserving information regarding subjects that could be of general interest or highly specialized.

- **Online Document Sharing and Collaboration** - Cloud-based software used to create, convert, or edit documents. Collaboration and sharing features may be available with access permissions typically configured by the author.

- **Private IP Addresses as Host** - Private IP addresses which are used as the host part of a URL. Private IP addresses are meant for internal use behind border routers only, so they are not publicly routable.

- **Terrorism and Violent Extremism** - Terrorist or extremist websites that promote death or violence as part of their ideology.

- **URL Shorteners**: Domains used to shorten long URLs, brand URLs, or may obscure the final destination of a hyperlink.

- **Web Cache and Archives**: Cached or archived web content often stored for preservation or to decrease load times.

Four new regionally restricted URL categories added:

- Great Britain

- Italy

- Germany

- Poland

Note The new regionally restricted URL categories: are added to help users address restrictions that maybe legally required by specific countries.

Note The regionally restricted categories are applicable to Cisco Web Security appliance versions that support multiple category verdicts.

Two existing URL categories are split into four new URL categories:

- Health and Nutrition split into:

  – **Recipes and Food**: Sites dedicated to sharing or discussing information about cooking, recipes, and food or non-alcoholic beverages; cultural aspects of cuisine and food; diet descriptions and adherence tips, general nutrition information about foods.

  – **Health and Medicine**: Health care; diseases and disabilities; medical care; hospitals; doctors; medicinal drugs; mental health; psychiatry; pharmacology; exercise and fitness; physical disabilities; vitamins and supplements; sex in the context of health (disease and health care); tobacco use, alcohol use, drug use, and gambling in the context of health (disease and health care).

- Nature category split into:

  – **Nature and Conservation**: Sites related to natural resources; ecology and conservation; forests; wilderness; plants; flowers; forest conservation; forest, wilderness, and forestry practices; forest management (reforestation, forest protection, conservation, harvesting, forest health, thinning, and prescribed burning); agricultural practices (agriculture, gardening, horticulture, landscaping, planting, weed control, irrigation, pruning, and harvesting); pollution issues (air quality, hazardous waste, pollution prevention, recycling, waste management, water quality, and the environmental cleanup industry).

  – **Animals and Pets**: Information about domestic animals, livestock, service animals, pets and their care.

Note [For Cisco Secure Email Gateway only] If you have already configured the mail policies in your email gateway with the Nature and Health & Nutrition URL categories, make sure that you reconfigure your mail policies with the new URL categories specified above.

Note The new URL categories specified above will now be available while configuring access control by URL category.

For more information on the changes made to Cisco Talos's URL Category lists, see the Cisco Talos blog at https://blog.talosintelligence.com/2021/01/2021-changes-to-content-and-threat-categories.html.

Release Date

Release Date: April 3, 2019

Changes

New URL Category added:

- Not Actionable - Sites that have been inspected but are unreachable or do not have enough content to be assigned a category.

The new URL category specified above will now be available while configuring access control by URL category.

Release Date

Release Date: May 8, 2017

Changes

New URL categories added:

- Online Meetings - online meetings, desktop sharing, remote access, and other tools that facilitate multi-location collaboration.
- Paranormal - UFOs, ghosts, cryptid, telekinesis, urban legends, and myths.
- Personal VPN - Virtual Private Network (VPN) sites, or tools that are usually for personal use, which may or may not have been approved for corporate use.
- DIY Projects - guidance and information to create, improve, modify, decorate and repair objects, articles, without the aid of experts or professionals.
- Hunting - professional or sport hunting, gun clubs, and other hunting related sites.
- Military - military, armed forces, military bases, military organizations, anti-terrorism.

This is the only change in this release. The six new URL categories specified above will now be available while configuring access control by URL category.

Threat Category Updates

Release Date

Release Date: February 8, 2021

Changes

Five existing threat categories removed:

- Mobile Threats
- P2P Malware
- Potential DNS Rebinding
- Dynamic DNS
- DNS-Tunneling

✎

Note Dynamic DNS and DNS-Tunneling are converted to URL categories.

For more information on the changes made to Cisco Talos's Threat Category lists, see the Cisco Talos blog at https://blog.talosintelligence.com/2021/01/2021-changes-to-content-and-threat-categories.html.

Support

Related Documentation

See the chapter for URL categories in the user guides for AsyncOS for Cisco Web Security Appliances and Cisco Email Security Appliances:

http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html

http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html

Customer Support

Cisco TAC: Visit http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

For non-critical issues, you can also access customer support from the appliance. For instructions, see the User Guide or online help.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.