Application and Threat Content Release Notes

Version 443

Notes: 1. Exposed a new custom IPS Vulnerability signature context, file-elf-body, that detects Executable and Linkable Format (ELF) files running over HTTP.

2. Google Hangouts will be shipping in next week's content release (July 1st). Google Hangouts is an instant messaging and video chat platform that replaces the following messaging products – Talk, Google+ Messenger and Hangouts, a video chat system within Google+ and some capabilities of Google Voice. Applications previously identified as google-talk, google-talk-gadget,gtalk-p2p,gtalk-voice,gmail-chat, gmail-video-chat will now be identified as one of the three applications under the google hangouts container- google-hangouts-base, google-hangouts-audio-video and google-hangouts-chat. The hangouts sub-applications would be identified as google-hangouts-base when Decryption is not enabled. With the new content release, security policies, specifically with rules to allow any of the previous google instant messaging services, must be updated with the appropriate hangouts application/s to ensure that they are not being blocked. Any existing application using the older Google services APIs would not be identified correctly unless updated with the latest hangouts APIs.

New Applications (4)

Risk	Name	Category	Subcategory	Technology	Depends On	Previously Identified As	Minimum PAN-OS Version
2	fcc-speed-test	general-internet	internet-utility	browser-based	flash,web-browsing	unknown-udp,unknown-tcp,web-browsing	3.1.0
2	intersystems-cache	business-systems	database	client-server	web-browsing	web-browsing/unknown-tcp	3.1.0
2	streetchat	collaboration	social-networking	client-server	apple-maps,cinemagram,ssl,web-browsing	web-browsing,ssl	3.1.0
1	tinder	collaboration	social-networking	client-server	apple-maps,facebook,ssl,web-browsing	web-browsing,ssl	3.1.0

Modified Applications (9)

Risk	Name	Category	Subcategory	Technology	Depends On	Minimum PAN-OS Version
3	citrix	networking	remote-access	client-server	socks,ssl,web-browsing	3.1.0

2	hipchat	collaboration	instant-messaging	client-server	jabber,rtmfp,ssl,web-browsing	3.1.0
1	hp-data-protector	business-systems	storage-backup	client-server		3.1.0
2	meetup-forum(function)	collaboration	web-posting	browser-based	meetup,ssl,web-browsing	3.1.0
1	rmi-iiop	business-systems	general-business	client-server		3.1.0
5	skype	collaboration	voip-video	peer-to-peer	msn,ssl,web-browsing	3.1.0
2	snapchat	collaboration	instant-messaging	client-server	google-app-engine,ssl,web-browsing	3.1.0
1	viber-base(function)	collaboration	voip-video	client-server	ssl,web-browsing	3.1.0
1	viber-voice(function)	collaboration	voip-video	client-server	ssl,viber	3.1.0

Modified Decoders (2)

Name
msrpc
ssl

New Anti-spyware Signatures (1)

Severity	ID	Attack Name	Default Action	Minimum PAN-OS Version	Maximum PAN-OS Version
critical	13469	MICROS0FT.AUTH Command and Control Traffic	alert	3.1.0	

Modified Anti-spyware Signatures (2)

Severity	ID	Attack Name	Default Action	Minimum PAN-OS Version	Maximum PAN-OS Version
critical	13457	Ebury SSH Rootkit Command and Control Traffic	alert	3.1.0	
high	20000	Conficker DNS Request	alert	3.0.0	4.1.0.0

New Vulnerability Signatures (3)

Severity	ID	Attack Name	CVE ID	Vendor ID	Default Action	Minimum PAN-OS Version
critical	36498	Malicious Flash file Detection			alert	4.0.0
critical	36505	Adobe Flash Player	CVE-2014-0536	APSB14-16	alert	4.0.0

		Memory Corruption Vulnerability				
critical	36506	Adobe Flash Player Memory Corruption Vulnerability	CVE-2014-0536	APSB14-16	alert	4.0.0

Modified Vulnerability Signatures (4)

Severity	ID	Attack Name	CVE ID	Vendor ID	Default Action	Minimum PAN-OS Version
critical	34886	Apple iTunes m3u Playlist File Title Parsing Buffer Overflow Vulnerability	CVE-2012-0677		alert	3.1.0
critical	36341	Microsoft Internet Explorer Memory Corruption Vulnerability	CVE-2014-0289	MS14-010	alert	4.0.0
high	36441	Apple Quicktime ftab Movie Atom Parsing Buffer Overflow Vulnerability	CVE-2014-1246		alert	5.0.0
high	35583	RealNetworks RealPlayer URL StringOverflow Vulnerability	CVE-2012-5691		alert	5.0.0