

UNCLASSIFIED



PALO ALTO NETWORKS STIG REVISION HISTORY

24 January 2024

Developed by DISA for the DOD

UNCLASSIFIED

REVISION HISTORY		
Document Revised	Description of Change	Release Date
- Palo Alto Networks ALG STIG, V2R3	<p>Palo Alto Networks ALG STIG, V2R4:</p> <ul style="list-style-type: none"> - PANW-NM-000047 - Added clarification for why DOD requires zone protection on the egress interface. Updated requirement to clarify that this is protecting against the DOD system being used to launch an attack on external systems. - PANW-AG-000102 - Updated requirement to clarify comply with https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVkCAK, and clarified the difference between this requirement and PAN-AG-000047. - Revision History format for multipart STIGs revised to ensure clarity in the versioning. 	24 January 2024

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
V2R4	- Palo Alto Networks NDM STIG, V2R1	<p>NDM STIG, V2R2</p> <ul style="list-style-type: none"> - PANW-NM-000075 - Corrected the check and fix to address the requirement that the neither the SA nor the Cryptographic Administrator can be the Audit Administrator. 	27 October 2022
	- Palo Alto Networks ALG STIG, V2R2	<p>ALG STIG, V2R3</p> <ul style="list-style-type: none"> - PANW-AG-000148 - Updated to reflect this is not a finding if the protocol is not used in the implementation. 	
	- Palo Alto Networks IDPS STIG, V2R2	<p>IDPS STIG, V2R3</p> <ul style="list-style-type: none"> - PANW-IP-000033 - Updated check and fix method for creating the vulnerability profile. 	
V2R3	- Palo Alto Networks NDM STIG, V1R4	- DISA migrated the Palo Alto Networks NDM STIG to a new content management system. The new content management system renumbered all Groups (V-numbers) and Rules (SV-numbers). With the new Group and Rule	27 April 2022

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<p>numbers, DISA incremented the version numbers from V1R4 to V2R1.</p> <p>Palo Alto Networks NDM STIG, V2R1 - PANW-NM-000023, PANW-NM-000042, PANW-NM-000054, PANW-NM-000062, PANW-NM-000063 - Requirement was removed from parent SRG. - PANW-NM-000075, PANW-NM-000092, PANW-NM-000096, PANW-NM-000098, PANW-NM-000099, PANW-NM-000110, PANW-NM-000114, PANW-NM-000143 - Updated CCI information.</p> <p>Palo Alto Networks ALG STIG - No updates this quarter.</p> <p>Palo Alto Networks IDPS STIG - No updates this quarter.</p>	
V2R2	<p>- Palo Alto Networks ALG STIG, V2R1</p> <p>- Palo Alto Networks IDPS STIG, V2R1</p>	<p>- PANW-AG-000102 - Updated discussion, added a new finding statement to check, and updated fix.</p> <p>- PANW-IP-000007 - Removed FQDN as an option in the fix text for consistency with the check and discussion.</p> <p>- PANW-IP-000020 - Changed all AV PA STIGs to state: If the "Action" is anything other than "drop" or "reset-both", this is a finding.</p>	23 July 2021
V2R1	<p>- Palo Alto Networks STIGs</p> <p>- Palo Alto Networks ALG STIG, V1R5</p>	<p>- DISA migrated the Palo Alto Networks STIGs to a new content management system. The new content management system renumbered all Groups (V-numbers) and Rules (SV-numbers). With the new Group and Rule numbers, DISA incremented the version numbers from V1R4 and V1R5 to V2R1.</p> <p>Palo Alto Networks ALG:</p>	23 October 2020

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
	- Palo Alto Networks IDPS STIG, V1R4	<p>PANW-AG-000062, PANW-AG-000063, PANW-AG-000073, PANW-AG-000074 - Changed check and fix action. Changed "Action" setting value to "drop" or "reset-both".</p> <p>Palo Alto Networks IDPS:</p> <p>- PANW-IP-000008 - Added note to fix text that this will only capture the first packet.</p> <p>No updates this release:</p> <p>- Palo Alto Networks NDM STIG, V1R4</p>	
V1R6	<p>- Palo Alto Networks STIG</p> <p>- Palo Alto Networks ALG STIG, V1R4</p> <p>- Palo Alto Networks IDPS STIG, V1R3</p> <p>- Palo Alto Networks NDM STIG, V1R3</p>	<p>- Combined ALG, IDPS, and NDM STIGs into one STIG package.</p> <p>Palo Alto Networks ALG:</p> <p>- V-62579, V-62581 - Revised content to use either Drop or reset-both.</p> <p>Palo Alto Networks IDPS:</p> <p>- V-62651 - Changed the wording to allow the info level to be omitted when packet captures are needed.</p> <p>- V-62661, V-62647 - Revised to use either Drop or reset-both.</p> <p>- V-62663 – Modified requirement to replace SCA with SA in rule title.</p> <p>Palo Alto Networks NDM:</p> <p>- V-62765 - According to the NIST evaluation, if the Palo Alto is in Common Criteria mode (configured to use NIST FIPS 140-2 modules for cryptographic functions), it will use HTTP OCSP with TLS. Revised text to reflect this.</p>	24 January 2020
V1R5	- Palo Alto Networks IDPS STIG, V1R2	<p>Palo Alto Networks IDPS:</p> <p>- V-62677 - Changed fix text to: In the "Source" tab, for "Zone", select the "External zone, for Source Address", select "Any". In the "Destination" tab, "Zone", select "Internal zone, for Destination Address", select "Any".</p>	25 October 2019

[illegible]

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
	- Palo Alto Networks NDM STIG, V1R2	<p>Palo Alto Networks NDM:</p> <ul style="list-style-type: none"> - Updated V-62721 fips-mode commands in check and fix to either add a note that they have changed in later version or change the commands to reflect current command sequence. <p>No updates this release:</p> <ul style="list-style-type: none"> - Palo Alto Networks IDPS STIG, V1R1 	
V1R2	- Palo Alto Networks ALG STIG, V1R1	<p>Palo Alto Networks ALG:</p> <ul style="list-style-type: none"> - Updated V-62603 fix to indicate that threat name field is a free-text entry field. - Updated V-62549, V-62551, V-62553, V-62633, and V-62635 to add a check and fix for PAN OS 7.0. - Updated V-62601 to remove second sentence in the vulnerability discussion and to correct fix (zones are reversed). - Updated V-62561 to correct the check, fix, and vulnerability discussion. - Updated V-62567 check and fix to correct the Packet Based Attack Protection options. - Updated V-62577 fix to include a manual process. - Updated V-62579 check to change "affects" to "allows" in the sentence, "For any Security Policy that affects traffic between Zones (interzone), view the "Profile" column." - Updated V-62593 to remove the last two sentences from the vulnerability discussion to improve clarity. - Updated V-62595 to remove the last two sentences from the vulnerability discussion to improved clarity. - Updated V-62597 in the check to state, "Go to Device >> Log Settings >> System". - Updated V-62627 to correct check and fix to include zone protection. 	22 July 2016

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
	- Palo Alto Networks NDM STIG, V1R1	Palo Alto Networks NDM: - Updated V-62773 check to exclude the emergency administration account. No updates this release: - Palo Alto Networks IDPS STIG, V1R1	
V1R1	- N/A	- Initial Release	01 December 2015