PALO ALTO NETWORKS
STIG REVISION HISTORY

27 April 2022

Developed by DISA for the DoD

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
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 numbers, DISA incremented the version numbers from V1R4 to V2R1. **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. **Palo Alto Networks ALG STIG** - No updates this quarter. **Palo Alto Networks IDPS STIG** - No updates this quarter.	27 April 2022
V2R2	- Palo Alto Networks ALG STIG, V2R1 - Palo Alto Networks IDPS STIG, V2R1	- PANW-AG-000102 - Updated discussion, added a new finding statement to check, and updated fix. - PANW-IP-000007 - Removed FQDN as an option in the fix text for consistency with the check and discussion. - 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.	23 July 2021
V2R1	- Palo Alto Networks STIGs	- DISA migrated the Palo Alto Networks STIGs to a new content management system. The new content management	23 October 2020

REVISION HISTORY

Revision Number	Document Revised	Description of Change	Release Date
	- Palo Alto Networks ALG STIG, V1R5 - Palo Alto Networks IDPS STIG, V1R4	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. **Palo Alto Networks ALG:** 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”. **Palo Alto Networks IDPS:** - PANW-IP-000008 - Added note to fix text that this will only capture the first packet. **No updates this release:** - Palo Alto Networks NDM STIG, V1R4	
V1R6	- Palo Alto Networks STIG - Palo Alto Networks ALG STIG, V1R4 - Palo Alto Networks IDPS STIG, V1R3 - Palo Alto Networks NDM STIG, V1R3	- Combined ALG, IDPS, and NDM STIGs into one STIG package. **Palo Alto Networks ALG:** - V-62579, V-62581 - Revised content to use either Drop or reset-both. **Palo Alto Networks IDPS:** - V-62651 - Changed the wording to allow the info level to be omitted when packet captures are needed. - V-62661, V-62647 - Revised to use either Drop or reset-both. - V-62663 – Modified requirement to replace SCA with SA in rule title. **Palo Alto Networks NDM:** - 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	24 January 2020

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		functions), it will use HTTP OCSP with TLS. Revised text to reflect this.	
V1R5	- Palo Alto Networks IDPS STIG, V1R2	**Palo Alto Networks IDPS:** - 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". **No updates this release:** - Palo Alto Networks ALG STIG, V1R3 - Palo Alto Networks NDM STIG, V1R3	25 October 2019
V1R4	- Palo Alto Networks ALG STIG,V1R3 - Palo Alto Networks IDPS STIG, V1R1	**Palo Alto Networks ALG:** - V-62571 - Updated the Vulnerability Discussion, Check content, and Fix text removed incorrect steps with steps to add anti-spoofing for IP to each zone policy. - V-62579 - In the Check content and Fix text changed "block" to "drop". Block is not a selection on this screen. - V-62581 - In the Vulnerability Discussion, Check content, and Fix text changed "block" to "drop". Block is not a selection on this screen. - V-62585 - In the Rule, Vulnerability Discussion, Check content, and Fix text changed "block" to "drop". Block is not a selection on this screen. - V-62587 - In the Vulnerability Discussion, Check content, and Fix text changed "block" to "drop". Block is not a selection on this screen. **Palo Alto Networks IDPS:** - V-62657 and V-62661 - In the Rule, Vulnerability Discussion, Check content, and Fix text change "block" to "drop". Block is not a selection on this screen. **No updates this release:**	25 January 2019

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- Palo Alto Networks NDM STIG, V1R3	
V1R3	- Palo Alto Networks ALG STIG, V1R2 - Palo Alto Networks NDM STIG, V1R2	**Palo Alto Networks ALG:** - Updated V-62549, V-62551, V-62553, V-62633, and V-62635 – Updated fips-mode commands in check and fix to add a reference to fips-cc command, which is used in later version. These versions were not the tested versions that are in scope for this document. Please note that minor updates cannot accommodate major changes in the software. **Palo Alto Networks NDM:** - 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. **No updates this release:** - Palo Alto Networks IDPS STIG, V1R1	28 July 2017
V1R2	- Palo Alto Networks ALG STIG, V1R1	**Palo Alto Networks ALG:** - 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."	22 July 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
	- Palo Alto Networks NDM STIG, V1R1	- 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. **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