

UNCLASSIFIED



PALO ALTO NETWORKS STIG REVISION HISTORY

24 January 2020

Developed by DISA for the DoD

UNCLASSIFIED

| REVISION HISTORY | | | |
|------------------|--------------------------------------|---|-----------------|
| Revision Number | Document Revised | Description of Change | Release Date |
| V1R5 | Palo Alto Networks STIG | - Combined ALG, IDPS, and NDM STIGs into one STIG package. | 24 January 2020 |
| V1R4 | - Palo Alto Networks ALG STIG, V1R4 | Palo Alto Networks ALG - V-62579, V-62581 - Revised content to use either Drop or reset-both. | |
| V1R4 | - Palo Alto Networks IDPS STIG, V1R3 | 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. | |
| V1R4 | - Palo Alto Networks NDM STIG, V1R3 | Palo Alto Networks NDM - V-62765 - According to the NIST eval, 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. | 25 October 2019 |
| V1R5 | - Palo Alto Networks STIG, V1R4 | 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". | |
| V1R4 | - Palo Alto Networks STIG, V1R3 | 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 | 25 January 2019 |

| REVISION HISTORY | | | |
|------------------|---------------------------------|---|--------------|
| Revision Number | Document Revised | Description of Change | Release Date |
| | | <p>changed "block" to "drop". Block is not a selection on this screen.</p> <p>- V-62585 - In the Rule, Vulnerability Discussion, Check content, and Fix text changed "block" to "drop". Block is not a selection on this screen.</p> <p>- V-62587 - In the Vulnerability Discussion, Check content, and Fix text changed "block" to "drop". Block is not a selection on this screen.</p> <p>Palo Alto Networks IDPS</p> <p>- 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.</p> | |
| V1R3 | - Palo Alto Networks STIG, V1R2 | <p>Palo Alto Networks ALG</p> <p>- Updated V-62549, V-62551, V-62553, V-62633, and V-62635 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.</p> <p>Palo Alto Networks NDM</p> <p>- 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> | 28 July 2017 |
| V1R2 | - Palo Alto Networks STIG, V1R1 | <p>Palo Alto Networks ALG</p> <p>- Updated V-62603 fix to indicate that threat name field is a free-text entry field.</p> <p>- Updated V-62549, V-62551, V-62553, V-62633, and V-62635 to add a check and fix for PAN OS 7.0.</p> <p>- Updated V-62601 to remove second sentence in the vulnerability discussion and to correct fix (zones are reversed).</p> | 22 July 2016 |

| REVISION HISTORY | | | |
|------------------|------------------|---|------------------|
| Revision Number | Document Revised | Description of Change | Release Date |
| | | <ul style="list-style-type: none"> - 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. <p>Palo Alto Networks NDM</p> <ul style="list-style-type: none"> - Updated V-62773 check to exclude the emergency administration account. | |
| V1R1 | - N/A | - Initial Release | 01 December 2015 |