Incident Report – Content version 578 on PA-3000 series devices

Incident Summary and Timeline:

At 20:10 PDT on 12-Apr-2016, Palo Alto Networks released its weekly Applications and Threat Content version 578. Within hours of this content version being available, we received reports that PA-3000 series devices that downloaded and installed this content version were dropping network traffic for various applications, including HTTP and HTTPS.

We would like to sincerely apologize to all our customers who were affected by this issue. We remain available to help resolve and remediate the problems caused by this content update on PA-3000 series devices, and to answer any questions you may have about this incident.

In an effort to address these critical issues reported by our customers, we removed this version of content from our update servers at 02:54 PDT on 13-Apr-2016, approximately 6 hours after the update was released. We took this step to ensure that PA-3000 series devices that had not yet downloaded and installed the content would not be affected by this issue. On the affected devices, the observed issue was remedied by reverting to content version 577 or earlier, thereby allowing the PA-3000 series firewalls to resume operational status. In addition, we sent out a notice to all customers registered for content update emails advising them to remain on content version 577 or earlier. In all reported cases, reverting to Applications and Threat Content release 577 addressed this issue.

Application and Threat Content update 579 was released at 20:25 PDT on 16-Apr-2016 to resolve issues caused by content version 578.

Incident Analysis and FAQ

Q: Why did this happen? Did Palo Alto Networks perform a root cause analysis for this issue?

Our hardware platforms drive network traffic through dedicated processing units that perform security processing functions. The PA-3000 series devices use a specific set of processing units to provide App-ID and Content-ID capabilities. Content version 578 caused these devices to hit a memory resource limit within one of the pattern-matching engines in these processing units, thereby causing the decoders used by App-ID and Content-ID to run out of resources. This, in turn, caused the PA-3000 series firewalls to discard sessions within these decoders, resulting in a network outage for these applications.

Root cause analysis indicates that a change introduced in content version 578 to the “msrpc” decoder is responsible for triggering this issue.

Q: Were platforms other than the PA-3000 series affected by this issue?

No. This issue is constrained to the PA-3000 series platforms only.

Q: Has this issue been resolved?

Yes. We released Application and Threat Content version 579 at 20:25 PDT on 16-Apr-2016 to address this issue. This update resolves the resource exhaustion issue seen on PA-3000 series devices that were running content version 578.

Q: What is Palo Alto Networks doing to prevent this from happening again?

We are adding new procedures and strengthening existing ones to measure, monitor, and verify a new content update, in terms of both process and technology.

Security processors will be specifically examined for resource exhaustion, to ensure that this issue is identified within our QA processes. Process changes are being introduced to check the impact of a new content version to ensure that any resource-related constraints are identified and fixed before releasing new content. We are also working to introduce technology changes that create a fallback mechanism on any firewall that encounters similar resource exhaustion issues.