AĞ GÜVENLİK CİHAZI KULLANMA KILAVUZU
MARKA: CİSCO
MODELLER: TG5004

GENEL BAKIŞ

Yerinde cihaz

Verilerin gizliliğini korumak için güvenli ve yüksek güvenlikli şirket içi statik ve dinamik kötü amaçlı yazılım analizi sağlar. Mevcut güvenlik altyapısı ile kolayca bütünleşir. Kötü amaçlı yazılım analizi sonuçlarının şirket içinde güvenli bir şekilde depolanmasını sağlar.

Gelişmiş analitik

AMP Threat Grid'in kapsamlı veritabanında, kötü amaçlı yazılım davranışları hakkında kapsamlı bir bilgi ve doğrudan örnekleme kaynağına ve ilişkili davranışa ilişkin bağlantılar sunar. Daha fazla araştırma için tüm bilgilere ve analiz sonuçlarına kolay erişim sağlar.

Gelişmiş davranış göstergeleri

Birkaç yanlış pozitif ile son derece hassas ve işlem yapılabilir ileri davranışsal göstergeleri analiz eder. Çok sayıda kötü amaçlı yazılım ailesini ve kötü niyetli davranışı içeren gelişmiş statik ve dinamik analizler yoluyla kapsamlı göstergeler üretir.

Tehdit puanı

Tehlike puanlarını tescilli analizlerden ve gözlemlenen eylemlerin, tarihsel verilerin, sıklık ve kümelenme göstergelerinin ve örneklerinin güven ve ciddiyetini dikkate alan algoritmalardan otomatik olarak türetir. Her numunenin kötü niyetli davranış seviyesini yansıtmak için tehditlere güvenle öncelik verir.

İçgörü #	TG5004-K9
MFR. #	TG5004-K9
UNSPSC:	43222501

Ürün Özellikleri

Genel	
Cihaz tipi	Güvenlik cihazı
Yükseklik (Raf Üniteleri)	1U
Genişlik	16.9 inç
Derinlik	29,8 inç
Yükseklik	1.7 inç

İşlemci / Bellek / Depolama	
Yüklenen İşlemciler	2 x Intel Xeon 2.3 GHz
Veri deposu	512 GB DDR4 SDRAM DIMM 288-pinli
Sabit disk	SSD 120 GB x 2 - SATA 6 Gb / s - 2,5 "
Sabit Sürücü (2.)	HDD - 1,2 TB x 6 - SATA 6 Gb / sn / SAS 12 Gb / sn
RAID Seviyesi	RAID 0, RAID 1, RAID 5, RAID 6, RAID 50, RAID 60

Ağ	
Form faktörü	Rafa monte
Limanlar Adet	2
Bağlantı Teknolojisi	telli
Veri aktarım hızı	10 Gb / sn

Ağ	
Veri Bağlantısı Protokolü	10 Gigabit Ethernet
Performans	Analiz edilen maksimum dosya sayısı: günde 1500

Genişleme / Bağlantı	
Arayüzler	2 x 10 GBase-X - SFP +

Çevresel Parametreler	
Dk çalışma sıcaklığı	41 ° F
Maksimum çalışma sıcaklığı	95 ° F
Nem aralığı çalışma	% 10 - 90 (yoğunlaşmamış)

KURULUM

2.1 Yükseltme 2,1 sürümüne yükseltmeden önce 2.0.4 sürümünde olmanız gerekir.

2.0.4 Yükseltmesi 2.0.4 güncellemesini tamamlayabilmeniz için önce 1.4.6 veya daha yeni bir sürümde olmanız gerekir.

2.0 Yükseltme İlk önce, 2,0'dan önceki adım olan 1.4.6 yükseltmesini tamamlayın. 1.4.6 yükseltmesi tamamlandıktan sonra ve 2,0 yükseltmesine devam etmeden önce, aşağıdaki hatanın meydana gelip gelmediğini doğrulamak için Tehdit Izgarası Portalındaki bildirimleri kontrol edin:

Şekil 1 Veritabanı Yükseltme Başarılı Değil Uyarı

" Veritabanı Yükseltme - Başarılı Değil " mesajı, yeni bir cihazın
PostgreSQL'in beklenenden daha eski bir sürümünü çalıştırdığını ve otomatik veritabanı geçiş işleminin başarısız olduğunu gösterir.
Hata uyarısını görmüyorsanız, 2,0 yükseltme işlemine devam edebilirsiniz.

2.0 Yükseltmesi İçin Gereken Zaman Büyük bir ElasticSearch veritabanı ile 2,0 güncellemesinin birkaç saat kadar sürebileceğini lütfen unutmayın. Tamamlanmadan önce yükseltme işlemini kesmeyin, aksi halde destek düzeltmesi gerekebilir.
Devam etmekte olan bir yükseltme durumunu kontrol etmenin en iyi yöntemi konsoldan erişimdir.
1.4'ten Önce Bir Sürümden Yükseltme 1,4'ten önceki bir sürümden yükseltme yapıyorsanız, aşağıdaki Sürüm 1,4 için sürüm notlarındaki bölümü okuduğunuzdan emin olun. 1.0 + hotfix2 Güncellemesi Zorunludur 1,0 + düzeltmesi2, büyük dosyaların bozulmadan çalışabilmesi için güncelleme sisteminin kendisini düzelten zorunlu bir güncellemedir.
Güncellemeler yükleniyor
Threat Grid Appliance'ı daha yeni sürümlerle güncelleyebilmeniz için, ilk kurulum ve yapılandırma adımlarını, AMP Threat Grid Appliance Kurulum ve Konfigürasyon Kılavuzunda belirtilen şekilde tamamlamış olmalısınız.
AMP Threat Grid Appliance ürün belgeleri sayfası. Yeni Cihazlar: Eski bir sürümle birlikte gelen ve güncellemeleri yüklemek isteyen yeni bir Cihazınız varsa, ilk önce ilk yapılandırmayı tamamlamanız gerekir. Tüm Aletler yapılandırması tamamlanana kadar güncellemeleri uygulamayın. Cihaz güncellemeleri, lisans yüklenmediği sürece indirilmez ve Cihaz veritabanı dâhil olmak üzere tamamen yapılandırılmadıysa doğru şekilde uygulanamayabilir.

Tehdit Izgarası Uygulaması güncellemeleri OpAdmin Portalı aracılığıyla uygulanır.

Güncellemeler tek yönlüdür: daha yeni bir sürüme yükselttikten sonra önceki bir sürüme geri dönemezsiniz.
Güncellemeyi test etmek için analiz için bir örnek gönderin

Yapı Numarası / Sürüm Sürümü Arama Tablosu

Yapı numarası	Serbest bırakma versiyon	Yayın tarihi	notlar
2016.05.20160905202824.f7792890.rel	2.1.4	2016/09/05	Öncelikle ilgi İmalat
2016.05.20160811044721.6af0fa81.rel	2.1.3	2016/08/11	Çevrimdışı güncelleme destek anahtarı, M4 desteği siler
2016.05.20160715165510.baed88a3.rel	2.1.2	2016/07/15	
2016.05.20160706015125.b1fc50e5.rel-1	2.1.1	2016/07/06	
2016.05.20160621044600.092b23fc	2.1	2016/06/21	
2015.08.20160501161850.56631ccd	2.0.4	2016/05/01	2.1 için başlangıç noktası güncelleştirme. Olmalısın 2.0.4 yapmadan önce 2.1'e güncelleyin.
2015.08.20160315165529.599f2056	2.0.3	2016/03/15	AMP'yi tanıtıyor entegrasyon, CA mgmt, ve DNS'yi bölme
2015.08.20160217173404.ec264f73	2.0.2	2016/02/18	
2015.08.20160211192648.7e3d2e3a	2.0.1	2016/02/12	
2015.08.20160131061029.8b6bc1d6	v2.0	2016/02/11	Güncellemeyi 2.0.1'e zorla buradan
2014.10.20160115122111.1f09cb5f	v1.4.6	2016/01/27	İçin başlangıç noktası 2.0.4 güncelleme
2014.10.20151123133427.898f70c2	v1.4.5	2015/11/25	
2014.10.20151118154826.9af96403	v1.4.4		
2014.10.20151020111307.3f124cd2	v1.4.3		
2014.10.20150904134201.ef4843e7	v1.4.2		
2014.10.20150824161909.4ba773cb	v1.4.1		
2014.10.20150822201138.8934fa1d	v1.4		

Yapı numarası	Serbest bırakmak versiyon	Yayın tarihi	notlar
2014.10.20150805134744.4ce05d84	v1.3		
2014.10.20150709144003.b4d4171c	v1.2.1		
2014.10.20150326161410.44cd33f3	v1.2		
2014.10.20150203155143 + düzeltme1.b06f7b4f	v1.1 + hotfix1		
2014.10.20150203155142.b06f7b4f	v1.1		
2014.10.20141125162160 + düzeltme2.8afc5e2f	v1.0 + hotfix2		**Not:** 1.0 + düzeltme2 zorunlu bir güncellemedir güncelleştirmeyi düzelten sistemin kendisi yapabilmek olmadan büyük dosyaları işlemek kırma.
2014.10.20141125162158.8afc5e2f	v1.0		

Sürüm 2.1.4
9.5.2016 yayınlandı
Bu sürüm, donanım desteği ile ilgili sayısız sorunu, özellikle hava boşluklu cihazlara yazılım güncellemeleri için destek sağlamanın önkoşulları olan sorunları giderir.

Yeni özellikler
ElasticSearch servisinin aşırı yük altında olduğu senaryolar için artık izleme ve raporlama mevcuttur.

Hata düzeltmeleri
Hatalı servislerin otomatik olarak yeniden başlatılması desteği, geçici olarak devre dışı bırakılmak üzere yeterince sıklıkta başarısız olan servislere (bir gecikmeden sonra) uzatılır.
Yeniden başlatma işleminde gecikme nedeniyle bazı dâhili hizmetlerin başlayamayacağı bir senaryo ele alınmıştır.
Depolama aygıtı adı veya kimlik değişikliği artık sistemin başarılı bir şekilde önyüklenmesini engellemez.
Sistem silinmesi artık TG-5004-K9 ve TG-5504-K9 donanımında tam olarak desteklenmektedir.

Bilinen Sorunlar
Disk G / Ç çıkış grafikleri, müşteriye ait veriler yerine, yalnızca işletim sisteminin özel dosya sistemine okur ve yazar. Bu, başlangıçta tamamlandıktan sonra sistem kök dosya sistemiyle etkileşimi en aza indirecek şekilde yapıldığı için hiçbir G / Ç gösterilmemektedir.

Sürüm 2.1.3
11.11.2016
Bu sürüm, donanım desteği ile ilgili sayısız sorunu, özellikle de hava alan cihazlara yazılım güncellemeleri için destek sağlamanın önkoşulları olan sorunları giderir.

Yeni özellikler
ElasticSearch servisinin aşırı yük altında olduğu senaryolar için artık izleme ve raporlama mevcuttur.

Hata düzeltmeleri

• Hatalı servislerin otomatik olarak yeniden başlatılması desteği, geçici olarak devre dışı bırakılmak üzere yeterince sıklıkta başarısız olan servislere (bir gecikmeden sonra) uzatılır.
• Yeniden başlatma işleminde gecikme nedeniyle bazı dâhili hizmetlerin başlayamayacağı bir senaryo ele alınmıştır.
• Depolama aygıtı adı veya kimlik değişikliği artık sistemin başarılı bir şekilde önyüklenmesini engellemez.
• Sistem silinmesi artık TG-5004-K9 ve TG-5504-K9 donanımında tam olarak desteklenmektedir.

Bilinen Sorunlar
Disk G / Ç çıkış grafikleri, müşteriye ait veriler yerine, yalnızca işletim sisteminin özel dosya sistemine okur ve yazar. Bu, başlangıçta tamamlandıktan sonra sistem kök dosya sistemiyle etkileşimi en aza indirecek şekilde yapıldığı için hiçbir G / Ç gösterilmemektedir

Sürüm 2.1.2

Çıkış tarihi: 7.15.2016

Bu küçük bir hata düzeltme sürümüdür.

Hata düzeltmeleri

• Temiz olmayan bir kapatma, sistemi redis anahtar / değer deposunun hizmet başlatmasını engellediği bir durumda artık bırakamaz.

• Qgu bağlantısındaki tg-tüneli bağlantısındaki gerileme (bu varsayılan olmayan özelliği kullanan müşteriler için) çözüldü.

• Bir sistemi artık tg-tüneli kullanmayacak şekilde değiştirmek artık otomatik bir işlemdir.

Bilinen Sorunlar

• Silme desteğinin, bazı özel BIOS sürümleriyle birlikte TG-5004-K9 ve TG-5504-K9 donanımında kırıldığı bilinmektedir. Bu donanımın piyasaya sürülmesinden önce çözülmesi bekleniyor.

• Disk G / Ç çıkış grafikleri, müşteriye ait veriler yerine, yalnızca işletim sisteminin özel dosya sistemine okur ve yazar. Bu başlangıçta tamamlandıktan sonra sistem kök dosya sistemiyle etkileşimi en aza indirecek şekilde yapıldığı için hiçbir G / Ç gösterilmemektedir.

Sürüm 2.1.1
Çıkış tarihi: 7.6.2016
Bu sürüm, ayrı bir temiz ağ DNS desteğindeki bazı sorunları giderir, önemli bir güvenlik hatasını giderir ve çeşitli küçük düzeltmeler ve geliştirmeler sağlar.

Yeni özellikler
• Potansiyel sabit sürücü arızalarına ilişkin SMART uyarıları kullanıcı tarafından görünürlük ayarlarında değişiklik yaparak susturulabilir ve bu da hatanın niteliği veya durumu değişinceye kadar aynı hatanın başka bildirimlerini önler.

Hata düzeltmeleri
• Ayrı temiz ağ DNS artık düzgün çalışıyor.
• Yeniden yapılandırma sonrası yedekleme sırasında yapılan sahte uyarılardan kaçınılır.

Güvenlik düzeltmeleri
• CVE-2016-1443 ele alınmıştır.
• SSH artık kurtarma modunda varsayılan olarak etkin değildir.
Bilinen Sorunlar
• Silme desteğinin, bazı özel BIOS sürümleriyle birlikte TG-5004-K9 ve TG-5504-K9 donanımında kırıldığı bilinmektedir. Bu donanımın piyasaya sürülmesinden önce çözülmesi bekleniyor.
• Disk G / Ç çıkış grafikleri, müşteriye ait veriler yerine, yalnızca işletim sisteminin özel dosya sistemine okur ve yazar. Bu, başlangıçta tamamlandıktan sonra sistem kök dosya sistemiyle etkileşimi en aza indirecek şekilde yapıldığı için hiçbir G / Ç gösterilmemektedir.

Sürüm 2,1
Çıkış tarihi: 6.21.2016
Önemli Not: Bu güncellemenin başlangıç noktası v2.0,4'tür.
Bu sürüm, yaklaşmakta olan donanım revizyonlarını tamamen destekler, sayısız güvenlik geliştirmeleri içerir ve Threat Grid Portal ürününün çağdaş sürümüne geçer.
Yeni özellikler

• Dosya türleri js, nokta, dotx ve DOTM şimdi kötü niyetli olarak gönderilebilir Dispozisyon Güncelleme Servisi ile FireAMP Özel Bulut.
• Güvenli Önyükleme yaklaşmakta olan TG-5004-K9 ve TG-5504-K9 donanımında çalışırken tam olarak desteklenmektedir.
• Tüm donanımlarda, modül yükleme ve kexec, çekirdek tabanlı rootkit'lere maruz kalmayı azaltmak için çalışma zamanında devre dışı bırakılır ve işletim sistemi çekirdeği ve initrd'nin imzaları, başlatma öncesinde önyükleyici tarafından doğrulanır.
• Sabit sürücü SMART uyarıları ile ilgili servis bildirimleri, yalnızca içerikleri değişirse otomatik olarak yeniden açılabilecek şekilde gizlenebilir.
• Uzun süre açık bırakılan veritabanı işlemleri, senaryo onarımı için uzatılmış aksama süresi gerektirecek kadar ciddi hale gelmeden önce düzeltmeyi destekleyen servis bildirimleri olarak algılanır ve raporlanır.
Hata düzeltmeleri
• Torpido gözünün güvenilirliği büyük ölçüde geliştirilmiştir.
• Ağ arabiriminin hazır olması için uzun bir süre gerektirdiği senaryolarda kurtarma modunda ağ güvenilirliği artırıldı.
• IPMI'nin donanım hatalarıyla ilgili servis bildirimleri hatalı olarak aktif uyarı sayısının 0 olduğunu iddia edebilir.
• NTP arızaları, sistem yapılandırması tamamlanmadan önce servis bildirimlerinin artmasına neden olmaz.
• Beklenen servislerin aktif olmaması nedeniyle oluşabilecek hatalar açılıştan en az 10 dakika öncesine kadar kaydedilemiyor, bu da servislerin doğru şekilde başlaması için zaman veriyor.
Güvenlik düzeltmeleri
• Temel sanallaştırma teknolojisi, VGA sürücüsündeki olası bir arabellek taşması için güncellenmiştir.
Bilinen Sorunlar
• Silme desteğinin, bazı özel BIOS sürümleriyle birlikte TG-5004-K9 ve TG-5504-K9 donanımında kırıldığı bilinmektedir. Bu donanımın piyasaya sürülmesinden önce çözülmesi bekleniyor.
• Disk G / Ç çıkış grafikleri, müşteriye ait veriler yerine, yalnızca işletim sisteminin özel dosya sistemine okur ve yazar. Bu sık sık demek ki başlatma bittikten sonra sistem kök dosya sistemiyle etkileşimi en aza indirecek şekilde yapıldığı için hiçbir G / Ç gösterilmez.

Sürüm 2.0.4

Çıkış tarihi: 5.1.2016
Önemli Not: Bu güncellemenin başlangıç noktası v1.4,6'dır.
Bu sürüm sayısız güvenilirlik geliştirmeleri ve düzeltmeleri içermektedir.
Özellikle büyük miktarda veri içeren cihazlar için önyükleme sürelerinin daha yavaş olabileceğini unutmayın;
ancak, önyükleme süresindeki bu artış, önyüklemeden kısa bir süre sonra meydana gelebilecek birkaç hatayı giderir.
Yeni özellikler
• Şimdi e-posta uyarısı için yapılan SMTP bağlantıları, yerel olarak yapılandırılmış sertifika yetkililerinden faydalanabilir.
• Elden Çıkarma Güncelleme Servisi entegrasyonu iyileştirildi ve FireAMP Private Cloud sürüm 2.2.0 ile tamamen uyumlu.
Hata düzeltmeleri
• Cihaz artık kullanım endekslerini güncelliyor, böylece amaçlanan durumlarına uyuyorlar. Bu, tutarsız veya güncel olmayan bir endeks durumunun neden olabileceği, müşteriyi etkileyen birkaç sorunu giderir.
• Cihaz, bağımlı servislere başlamadan önce ElasticSearch kümesinin tamamen hazır olmasını bekler.
• ElasticSearch için ayrılan bellek miktarı ve böylece ElasticSearch'te hatasız endekslenebilecek maksimum veri miktarı arttırıldı.
• 1.x'ten 2.x'e yükseltme sırasında uygulananlar gibi geçici önyükleyici yapılandırması geçersiz kılmaları silindi. Sonuç olarak, kurtarma modu kullanımdayken, bir 1.x sürümünden daha önce yükseltilmiş bir cihaza bir yükseltme modu menüsü sunmasına neden olabilecek bir senaryo.
• E-posta uyarısının başarısız olmasına neden olabilecek bir hata giderildi.

Sürüm 2.0.3
Çıkış tarihi: 3.15.2016
Bu nokta sürümü, FireAMP Private Cloud cihaz entegrasyonlarını destekleyen bir dizi özellik sunar. Bunlar arasında DNS'yi Temiz ve Kirli arayüzler, CA Yönetimi ve FireAMP Entegrasyon Yapılandırması arasında bölme özelliği bulunur.

Üretilen SSL sertifikaları şimdi CN'nin bir topicAltName olarak çoğaltılmıştır. Bu, en az bir konuAltName olduğunda CN alanını yok sayan SSL istemcileriyle bir uyumsuzluğu giderir. Bu tür araçları kullanıyorsanız, daha önce cihazda üretilen sertifikaları yeniden oluşturmak gerekebilir.

Sürüm 2.0.2
Çıkış Tarihi 2.18.2016
Yalnızca bu hata düzeltme sürümü, acil bir güvenlik sorununu giderir.

Güvenlik güncellemeleri
GNU C Kütüphanesi CVE-2015-7547 ve CVE-2015-1781'e yönelik olarak eklenmiştir.

Sürüm 2.0.1
Çıkış Tarihi 02.12.2016
Yalnızca bu hata düzeltme sürümü, 2,0'da bulunan bazı sorunları düzeltir.

Hata düzeltmeleri
Bir cihazın kotasını kontrol etme çağrıları artık o kotaya göre sayılmaz.
Bir cihazın açılışta askıda kalmasına neden olabilecek bir sorun çözüldü.

Bilinen Sorunlar
Disk G / Ç çıkış grafikleri, müşteriye ait veriler yerine, yalnızca işletim sisteminin özel dosya sistemine okur ve yazar. Bu, başlangıçta tamamlandıktan sonra sistem kök dosya sistemiyle etkileşimi en aza indirecek şekilde yapıldığı için hiçbir G / Ç gösterilmemektedir.

Sürüm 2,0
Çıkış Tarihi 2.11.2016
Önemli Not: Güncellemeyi buradan 2.0.1'e zorlayın.
Bu, güncellenmiş bir işletim sistemine dayanan önemli bir sürümdür.
Gelecekteki donanım sürümlerini destekleyen ve Threat Grid Cloud Portal ürünüyle aynı yazılımı kullanabilecek geliştirmeleri içerir.
2.0 yükseltme işleminin büyük bir ElasticSearch veritabanıyla birkaç saat kadar sürebileceğini lütfen unutmayın.
Tamamlanmadan önce yükseltme işlemini kesmeyin, aksi halde destek düzeltmesi gerekebilir.
Devam etmekte olan bir yükseltme durumunu kontrol etmenin en iyi yöntemi konsoldan erişimdir.
Aşağıdaki Tehdit Izgarası Cihazına özel güncellemeler de dâhil edilmiştir:

Yeni özellikler
• Windows 7 64 bit VM'ler artık desteklenmektedir.
• Müşteri desteği tarafından başlatılan izler artık otomatik olarak döndürülmekte ve silinmektedir, bu nedenle mevcut alanı tüketme riski olmadan daha uzun süre çalışabilirler.
• Dahili konfigürasyon yedekleri daha ayrıntılı olup, her iki SSD'nin de başarısız olması durumunda bile bir cihazın büyük veri kaybı olmadan kurtarılmasını sağlar.

Hata düzeltmeleri
• Kimliği doğrulanmamış SMTP, kimlik doğrulama işlemini boş bir yöntem listesiyle (özellikle Microsoft Exchange) ilan eden posta sunucularında bile düzgün çalışır.
• Gecelik güncellemeler indirme sırasındaki arızalarla ilgili servis bildirimleri şimdi doğru bir şekilde teslim edildi.
Güvenlik düzeltmeleri
• Hesap oluşturma veya CSA cihazı (yani, ESA / WSA / vb.) Kaydıyla ilgili uygulama düzeyinde bildirimler, nbildirim uyarıları için yapılandırılmış ilk e-posta adresine gönderilir . Hiçbir adres yapılandırılmazsa, bildirimler gönderilmez.
(Önceki sürüm sürümleri bu bildirimleri admin@test.threatgrid.com adresine göndererek potansiyel olarak veri sızıntısına neden olabilir.)
• OpenSSL 1,0.2f sürümüne güncellendi.
Bilinen Sorunlar
Disk G / Ç çıkış grafikleri, müşteriye ait veriler yerine, yalnızca işletim sisteminin özel dosya sistemine okur ve yazar. Bu, başlangıçta tamamlandıktan sonra sistem kök dosya sistemiyle etkileşimi en aza indirecek şekilde yapıldığı için hiçbir G / Ç gösterilmemektedir.
Gelecek sürümler, G / Ç kullanımının bu soruna geçici bir çözüm bulmak için kullandığı yöntemi değiştirebilir.

1.4.6 Versiyonu
Çıkış
1.4.6 Sürümü, 2,0'a yükseltme sırasında kullanılan araçları yükler.
Yeni özellikler
1.4.6 sürümündeki cihazlar, 2,0 sürümüne yükseltilmeye uygundur.

1.4.5 Versiyonu
2015.11.25

Cihazı Sil özelliği artık 1.4.4 ile birlikte gelen demo cihazlarda işlevseldir. Daha fazla bilgi için, lütfen "Cihaz Silme" bölümüne bakın.

Sürüm 1.4.4
Bu sürüm, lisans doğrulamasını etkileyen kritik bir sorunu giderir ve gecelik güncelleme kontrolündeki hataların kullanıcıya sunulmasını önleyen bir hatayı giderir.

ÖNEMLİ: 1,4'ten önceki bir sürümden yükseltme yapıyorsanız, aşağıdaki 1,4 sürümü için sürüm notlarını mutlaka okuyun.

Hata düzeltmeleri

- Lisans doğrulaması artık salt okunur bir iç veritabanını yeniden kurma girişiminde bulunmaz (lisansların yanlışlıkla geçersiz olarak reddedilmesine neden olabilir).
- Gece güncelleme kontrolündeki hatalar artık kullanıcıya doğru bir şekilde gösteriliyor.

Sürüm 1.4.3
Bu sürüm, temel sanallaştırma altyapısı için küçük güvenlik güncellemeleri içerir ve bir cihazın disklerini silmek için kullanıcı tarafından erişilebilir bir mekanizma ekler (ödünç alınan donanımın Cisco Demo Kredi Programına geri verilmesi veya iadesi için).
Yeni özellikler
- Sil: Bir Tehdit Izgarası Uygulamasındaki diskleri silmenizi sağlayacak yeni bir önyükleme menüsü seçeneği mevcuttur.
Bu işlemi yaptıktan sonra, cihazın tekrar arama için Cisco'ya iade edilmeden çalışmayacağına dikkat edin.
Güvenlik güncellemeleri
- Çalışan numunelerin askıda kalmasına neden olmak için hazırlanmış Ethernet paketleri kullanan olası bir hizmet reddi artık mümkün değildir.
Bilinen Sorunlar
- Nadir durumlarda, Windows XP'deki VM analizinin başarısız olduğu biliniyor. Örnek analizine ait video, bu gerçekleştiğinde siyah bir ekran gösterecektir. Bu başarısızlık bireysel örneklemden bağımsızdır; bu olursa, numuneyi tekrar göndermek (veya Windows 7'ye geçmek) önerilir.

1.4.2 Versiyonu
Bu sürüm, üründe kullanılan temel sanallaştırma teknolojisini günceller ve birkaç küçük fakat önemli hata düzeltmesini içerir.

ÖNEMLİ: 1,4'ten önceki bir sürümden yükseltme yapıyorsanız, aşağıdaki 1,4 sürümü için sürüm notlarını mutlaka okuyun.

Hata düzeltmeleri
- Flash (SWF) belgeleri şimdi doğru şekilde etkinleştirildi.
- "Torpido gözü" aracındaki canlı örnek analizi çalışmalarıyla etkileşime geçme desteği, artık Firefox 40'taki yeni güvenlik varsayılanlarıyla uyumludur.
- "Yeniden Üret" düğmesi, daha önce bunları reddeden bazı yazılımlar ve araçlar için kabul edilebilir SSL sertifikaları oluşturur.
- Windows 7 sanal makineleri yürütme sırasında artık askıya alınmayacak.

Bilinen Sorunlar
- Nadir durumlarda, Windows XP'deki VM analizinin başarısız olduğu biliniyor. Örnek analizine ait video, bu gerçekleştiğinde siyah bir ekran gösterecektir. Bu başarısızlık bireysel örneklemden bağımsızdır; bu olursa, numuneyi tekrar göndermek (veya Windows 7'ye geçmek) önerilir.

Sürüm 1.4.1
Bu sürüm, üründe bulunan Windows 7 görüntüsünü güncelleyerek Microsoft Office etkinleştirme iletişim kutusunu engeller.

ÖNEMLİ: 1,4'ten önceki bir sürümden yükseltme yapıyorsanız, aşağıdaki 1,4 sürümü için sürüm notlarını mutlaka okuyun.

Hata düzeltmeleri
- Microsoft Office belgelerini Windows 7 kullanarak analiz ederken, Microsoft Office etkinleştirme iletişim kutusu artık görüntülenmiyor.
- Önyükleme işleminin başında sistem davranışının analizi için müşteri destek araçlarının kullanılması, bu araçlar artık etkin olmadığında artık bir servis uyarısıyla sonuçlanmamaktadır.

Sürüm 1,4

Bu sürüm, yaklaşmakta olan 2,0 sürümüne yükseltmeye hazırlanmak için gerekli olan depolama formatındaki değişikliklere odaklanmıştır.

ÖNEMLİ:
Başlangıçta 1,0 serisi bir yazılımla birlikte gelen ve büyük miktarda veritabanı içeriğine sahip cihazlar için bu yükseltme işlemi normalden daha uzun sürecek bir bakım penceresi gerektirebilir.

İlk olarak 1,2'den önce birkaç ay boyunca kullanılmakta olan bir yazılım sürümüyle birlikte gönderilen aygıtlar için, yükseltmenin uygulanması için 90 dakika beklemenizi öneririz.

1.0 öncesi (Cisco markalı olmayan) bir cihazdan örnek verileri aktarılan cihazlar için yükseltme işlemi daha uzun sürebilir; Lütfen sorularınız için müşteri desteğine başvurun.

Yeni özellikler
- Standart yukarı akış veritabanı sürümleriyle uyumlu bir PostgreSQL 9,4 yapısını kullanmak için tüm cihazlarda veritabanı depolamayı yükseltir.
- Yeni bir fonksiyonla tgsh-diyaloğuna UYGULAMA butonunu yeniden ekle: Kendinden konfigürasyon ve güncelleme görevlerini bir sistem güncellemesinden sonra yapıldığı şekilde tamamlar.
İptal edilen bir güncelleme girişiminden sonra tutarsız bir durumda bırakılmış bir sistemi onarmak için kullanılabilir.
- Müşteri desteğinin, diğer Cisco cihazları tarafından tetiklenen işler için kullanılan varsayılan sanal makineyi seçebileceği bir mekanizma eklendi.

Hata düzeltmeleri
- Yeni sanal makine görüntülerine sahip güncellemeler, sistem yazma performansı düşerse artık hataya açık değildir.
- Konsoldan çağrılan güncelleme işleri artık Opadmin'de başarısız olarak yanlış tanımlanmaya meyilli değildir.
- Yükseltme işlemi sırasında hizmet bildirimleri artık oluşturulmamaktadır.
- Bazı Microsoft Office belge türleri için oluşturulan hatalı dosya adı uzantıları düzeltildi.

Sürüm 1,3
Bu sürüm, aşağıdakiler dâhil, cihaza özgü önemli özellikler ekler: uzak syslog desteği; sistem düzeyinde sorunların e-postayla uyarılması ve performans grafiklerinin mevcudiyeti. Bu sürüm, Cisco FireSIGHT Management Center ürünleriyle entegrasyon için destek uygulayan ThreatGRID servisinin biraz daha yeni bir sürümüne geçti. Bu sürüm aynı zamanda cihaza özgü hata düzeltmelerini de içeriyor.

Uzak syslog'ların - eğer konfigüre edilmişse - giden trafik için temiz arayüzü kullandığını unutmayın. Daha fazla bilgi için lütfen 1,3 için güncellenmiş idari dokümana bakınız.

Yeni özellikler
- E-postayla gönderilen bildirimler, sistem izleme olaylarını tetikleyecek şekilde yapılandırılabilir.
- Yönetici arabiriminin SSL yapılandırma sayfasına eklenen düğme, kendinden imzalı yeni SSL sertifikaları oluşturur.
- Yönetici arayüzünde CPU, I / O ve zaman içindeki bellek kullanımı grafikleri bulunmaktadır.
- İşletim sistemi seviyesindeki ağ arayüzü adları artık
belgelerde kullanılan mantıksal adlarıyla ("temiz", "kirli", "yönetici") eşleşmektedir.
- Hotplugging ağ arayüzleri desteklenir; bir arayüzün
daha sonra çalışabilmesi için önyükleme sırasında takılı olması gerekmez ve hotplug olaylarında DHCP yenilemesi gerektiren arayüzler bunu yapar. (
SFP'ler gerektiren arayüzler hala önyüklemede kurulu olan SFP'lere sahip olmalıdır).
- Başarısız olan servisler otomatik olarak yeniden başlatılır.
- Hatalı servisler uygulamada servis bildirimleri oluşturur.
- NTP senkronizasyonundaki başarısız denemeler uygulamada servis bildirimleri üretir.
- Aşırı veritabanı denetim noktası birikintisi, kullanıcının görebileceği bir uyarıya neden olur.
- Boş alan etkinlikleri için bir servis bildirimi eklendi.
- Yükseltme kullanılabilirliği ile ilgili hizmet bildirimlerine sürüm notu içeriği eklendi.

Hata düzeltmeleri
- 24 bit / 24'ün üzerinde yüksek bitli ağ maskeleri artık erken kesilmez.

Güvenlik güncellemeleri
- CD-ROM sürücüsü aracılığıyla istismarları devre dışı bırakmak için qemu yamaları; CVE-2015-5154'e bakınız.
- Uygulama hata ayıklama arayüzleri aracılığıyla yerel imtiyaz artışı için fırsatlar hafifletildi.

Diğer notlar
- EULA şartları güncellendi.

Sürüm 1.2.1
Bu, ThreatGRID cihazını, bulut hizmetinin daha yeni bir sürümündeki yazılıma dayalı olacak şekilde günceller. Anahtar ESA ve WSA dahil - eklenen özellikler arasında diğer Cisco cihazları ile entegrasyon için destek aletleri.

Bu sürümde hiçbir cihaza özgü kod veya altyapı değiştirilmedi.

Yeni özellikler
- Cisco Sandboxing API desteği

Güvenlik güncellemeleri
- Yamaları QEMU disket denetleyicisi öykünmesini devre dışı bırakmak, CVE-2015-3456 kaçınarak

Sürüm 1,2
Bu nokta sürümü, diğer Cisco ürünleriyle entegrasyonu geliştirir, yazılım güncelleme işlemini kolaylaştırır ve donanım izleme desteği ekler.

Yeni özellikler
- Yazılım güncellemeleri kontrolleri artık gece bazında arka planda otomatik olarak gerçekleştiriliyor.
- Artık bir yazılım güncellemesi mevcut olduğunda Threat Grid uygulamasında bildirim sağlandı.

Hatalar düzeltildi
- Yazılım güncellemeleri yavaş bağlantılarda zaman aşımına uğradı.
- Bir kapatma veya yeniden başlatma sırasında işlenen örnekler artık kaybolmaz veya kopya olarak eklenmez. 1.2 güncellemesi uygulandıktan sonra, örnek işleme, işlem uygun bir durma noktasına ulaşana kadar kapanmayı geciktirir. Cihaz yeniden başlatıldığında örnek işleme devam eder. (Önceden, örnek işleme, sistem kapatmanın yanı sıra örneklerin kaybında daha uzun bir gecikmeye neden olabilir.)
- "502 Bad Gateway" hataları, cihaz açılırken artık oluşmuyor.
- NTP (Ağ Zaman Protokolü) senkronizasyonu şimdi doğru şekilde gerçekleşiyor.
- Üretilen SSL sertifikası seri numaraları artık tüm uygulamalar için benzersiz. ** NOT: ** Bu düzeltme yalnızca ilk olarak sürüm 1,2 veya daha yenisiyle kurulan sistemleri etkiler.
- Nispeten düşük sayıda numunenin işlenmesinden sonra cihazların disk alanından tükenmesine neden olan bir depolama yanlış konfigürasyonu düzeltildi.
- Denetim günlükleri şimdi doğru bir şekilde istemci IP adresini gösterir.
- SSH anahtar konfigürasyon sayfasındaki metin, bunun root değil, tehdit kullanan kullanıcı için anahtarları konfigüre ettiğini doğru şekilde yansıtır.
- Oluşturulan e-postalardaki parola sıfırlama bağlantıları artık doğru.

Güvenlik güncellemeleri
- Yönetici arayüzü için oturum çerezleri artık Threat Grid cihazlarında taşınabilir değildir.
- OpenSSL yukarı yöndeki düzeltmeleri içerecek şekilde yükseltilmiştir.

Diğer İyileştirmeler
- İlk sürüm 1,2 veya daha yenisiyle yüklü olan cihazlarda, PostgreSQL veritabanı, yukarı akış PostgreSQL ve EnterpriseDB gibi ilgili projelerle ikili uyumlu bir depolama formatı kullanır

Bilinen Sorunlar
- Windows 7 işleri çalıştırılmadan önce, aşağıdaki kullanıcı müdahalesi gerekir:

1. Temiz kullanıcı arabirimindeki birincil ThreatGRID uygulama konsoluna yönetici kullanıcısı olarak giriş yapın.

2. Açılır menüye erişmek için sağ üst köşedeki ** Welcome Admin ** düğmesine tıklayın.

3. ** Orgları Yönet ** seçeneğini tıklayın.

4. ** İlk Organizasyon ** seçeneğini tıklayın.

5. ** Ek VMS ** alanına ** win7 ** girin. 6. ** Güncelle ** düğmesine tıklayın.

Bu yapıldıktan sonra, bir örnek gönderirken, ** Gelişmiş Seçenekler ** altında, kullanıcı ** win7 ** 'yi seçebilir.

- Lisans ayrıştırma metin dosyası formatına duyarlıdır. Lisanslar UNIX metin dosyalarında saklanmalıdır - CRLF yerine CR ile sınırlandırılmış satırlarla.

Sürüm 1,1 Düzeltme 1
Düzeltme 1, 1,1 ile aynıdır, ancak yavaş bağlantılar üzerinden güncelleme indirme güvenilirliğini etkileyen bir hatayı düzeltir

Sürüm 1,1

Bu nokta sürümü, Tehdit Izgarası aracına (Pencere 7 desteği dâhil) birkaç yeni özellik ekler ve birkaç hatayı giderir.

Yeni özellikler

- Windows 7 desteği eklendi.

- E-posta, yalnızca
** Kirli ** (yani kötü amaçlı yazılım) arayüzü kullanılarak erişilebilen posta sunucularına izin vermek yerine, cihazın ** Temiz ** ağına bağlı posta sunucuları aracılığıyla gönderilebilir.

- Destek anlık görüntüleri doğrudan cihazdan Tehdit Izgarası Desteği'ne gönderilebilir.

- Destek anlık görüntüleri, Tehdit Izgarası Desteğine gönderilmeden önce görüntülenebilir.

- Güncellemeler, sadece web tabanlı yönetim arayüzünün (** OpAdmin **) aksine, metinsel (küfürler) arayüzünden uygulanabilir.

- Sistem şifresi kurtarma modundan başarıyla değiştirilebilir.

- Daha az idari değişiklik etkili olmak için yeniden başlatma gerektirir.

- GUI yapılandırma iş akışı için daha fazla istemci tarafı Javascript doğrulama eklendi.

Hatalar düzeltildi

- Giden e-posta yapılandırmasıyla ilgili çeşitli sorunlar çözüldü.

- Yönetici arayüzündeki bildirimler doğru şekilde görüntülendi.

- Yapılandırma kullanıcı arabiriminde uzun süredir devam eden işlerin durumu şimdi en az gecikmeyle yayınlandı.

- Yönetici arayüzünün başlamayı reddedebileceği bir durum düzeltildi.

- Konfigürasyon GUI, konfigürasyon değişikliklerinin
etkili olması için yeniden başlatmanın gerekip gerekmediğini her zaman tam olarak yansıtmamıştır. Bu giderildi.

- Desteklenmeyen menü öğelerini tgsh-dialog (curses tabanlı) yönetim arabiriminden kaldırıldı.

Güvenlik güncellemeleri

- Bilinen güvenlik açıkları olan yukarı akış paketleri güncellendi (ntpd, bash, openssl).

- Yapılandırma yedekleri artık dünyaca okunabilir durumda değil

BAKIM, ONARIM VE KULLANIMDA UYULMASI GEREKEN KURALLAR:

Ürünün kullanıcı tarafından yapılabilecek her hangi bir bakım ya da onarım işlemi bulunmamaktadır. Potansiyel zararlardan korunmak için cihazı, sıcaktan, sıvı temasından, nemden ve tozdan koruyunuz. Cihaz ısı kaynağından en az 30 cm uzak olmalıdır.

KULLANIM SIRASINDA İNSAN VEYA ÇEVRE SAĞLIĞINA TEHLİKELİ VEYA ZARARLI OLABİLECEK DURUMLARA İLİŞKİN UYARILAR:

Lütfen kullanım ömrü tamamlandığında elektronik çöp dönüşümü yapabilen yerlere ürünü teslim ediniz.

KULLANIM HATALARINA İLİŞKİN BİLGİLER:

Burada belirtilenler ile sınırlı olmamak kaydı ile bu bölümde bazı kullanıcı hatalarına ilişkin örnekler sunulmuştur. Bu ve benzeri konulara özen göstermeniz yeterlidir.
Örnekler:
Aleti çalışır durumda taşımak, temizlemek vb. eylemler Alet üzerine katı ya da sıvı gıda maddesi dökülmesi Aletin taşıma sırasında korunmaması ve darbe alması

TÜKETİCİNİN KENDİ YAPABİLECEĞİ BAKIM, ONARIM VEYA ÜRÜNÜN TEMİZLİĞİNE İLİŞKİN BİLGİLER:

Ürünün tüketici tarafından yapılabilecek bir bakım prosedürü bulunmamaktadır. Cihaz çalışır durum da iken temizlik yapmayınız. Islak bezle, köpürtülmüş deterjanlarla, sulu süngerlerle temizlik yapmayınız.

ÜRÜN HERHANGİ BİR PERİYODİK BAKIM ONARIM GEREKTİRMEMEKTEDİR.

MALIN ENERJİ TÜKETİMİ AÇISINDAN VERİMLİ KULLANIMINA İLİŞKİN BİLGİLER

Satın almış olduğunuz ürünün ömrü boyunca enerji tüketimi açısından verimli kullanımı için bakım hizmetlerinin yetkilendirilmiş sertifikalı elemanlarca yapılması gerekmektedir.

TAŞINMA ve NAKLİYE SIRASINDA DİKKAT EDİLECEK HUSUSLAR

- Paketlerken, orijinal kutusunu ve paketleme malzemelerini kullanın.
- Cihazı kullanırken ve daha sonra bir yer değişikliği esnasında sarsmamaya, darbe, ısı, rutubet ve tozdan zarar görmemesine özen gösteriniz.

TÜKETİCİNİN SEÇİMLİLİK HAKLARI

Malın ayıplı olduğunun anlaşılması durumunda tüketici, 6502 sayılı Tüketicinin Korunması Hakkında Kanunun 11 inci maddesinde yer alan;

a- Sözleşmeden dönme,

b- Satış bedelinden indirim isteme,

c- Ücretsiz onarılmasını isteme,

ç- Satılanın ayıpsız bir misli ile değiştirilmesini isteme, haklarından birini kullanabilir.

Tüketicinin bu haklardan ücretsiz onarım hakkını seçmesi durumunda satıcı; işçilik masrafı, değiştirilen parça bedeli ya da başka herhangi bir ad altında hiçbir ücret talep etmeksizin malın onarımını yapmak veya yaptırmakla yükümlüdür. Tüketici ücretsiz onarım hakkını üretici veya ithalatçıya karşı da kullanabilir. Satıcı, üretici ve ithalatçı tüketicinin bu hakkını kullanmasından müteselsilen sorumludur.

Tüketicinin, ücretsiz onarım hakkını kullanması halinde malın;

- Garanti süresi içinde tekrar arızalanması,

- Tamiri için gereken azami sürenin aşılması,

- Tamirinin mümkün olmadığının, yetkili servis istasyonu, satıcı, üretici veya ithalatçı tarafından bir raporla belirlenmesi durumlarında; tüketici malın bedel iadesini, ayıp oranında bedel indirimini veya imkân varsa malın ayıpsız misli ile değiştirilmesini satıcıdan talep edebilir. Satıcı, tüketicinin talebini reddedemez. Bu talebin yerine getirilmemesi durumunda satıcı, üretici ve ithalatçı müteselsilen sorumludur.

Tüketici, garantiden doğan haklarının kullanılması ile ilgili olarak çıkabilecek uyuşmazlıklarda yerleşim yerinin bulunduğu veya tüketici işleminin yapıldığı yerdeki Tüketici Hakem Heyetine veya Tüketici Mahkemesine başvurabilir.

AEEE YÖNETMELİĞİNE UYGUNDUR. 

İthalatçı Firma

TECH DATA BİLGİSAYAR SİSTEMLERİ A.Ş.

Saray Mahallesi, Site Yolu Sokak

Anel İş Merkezi No:5 Kat:8

Ümraniye, İstanbul,34768

Tel : +90 216 999 53 50

Üretici Firma

Cisco Systems, Inc.

170 West Tasman Drive San Jose, CA 95134-1706 USA http://www.cisco.com

Tel: 408 526-4000 800 553-NETS (6387) Fax: 408 527-0883