Інформація про безпеку TeamViewer

© TeamViewer GmbH, 2017. Останнє оновлення: 5/2017

Цільова аудиторія

Цей документ призначений для професійних адміністраторів мережі. Інформація в цьому документі дуже докладна й має радше технічний характер. На основі цієї інформації IT-спеціалісти отримають детальнішу картину стандартів безпеки в програмі TeamViewer та зможуть позбутися занепокоєнь ще до запуску нашого програмного забезпечення. Ви можете передавати цей документ своїм клієнтам, щоб усунути будь-які можливі проблеми, пов'язані з безпекою.

Якщо ви не вважаєте себе частиною цільової аудиторія, загальна інформація в розділі «Компанія/програмне забезпечення» допоможе отримати чітке уявлення про наше серйозне ставлення до безпеки.

Компанія/програмне забезпечення

Про нас

Компанія TeamViewer GmbH заснована у 2005 році в Південній Німеччині в місті Геппінген (поблизу Штутгарта) і має дочірні компанії в Австралії й США. Ми займаємося виключно розробкою та продажем систем безпеки для співпраці в Інтернеті. Протягом короткого періоду часу видача наших умовно-безкоштовних ліцензій призвела до швидкого зростання компанії: понад 200 млн користувачів програмного забезпечення TeamViewer, інстальованого на 1,4 млрд пристроїв більш ніж у 200 країнах світу. Програмне забезпечення доступне більш ніж 30 мовами.

Наша концепція безпеки

Програму TeamViewer щомиті застосовують понад 30 млн користувачів. Вони надають термінову підтримку через Інтернет, отримуючи доступ до автономних комп'ютерів (тобто забезпечують віддалену підтримку для серверів), і проводять онлайн-конференції. Залежно від конфігурації TeamViewer можна використовувати для віддаленого керування іншим комп'ютером, ніби ви працюєте безпосередньо за ним. Якщо користувач, який підключається до віддаленого комп'ютера, є адміністратором операційних систем Windows, Mac або Linux, на комп'ютері, у систему котрого він входить, йому також надаються права адміністратора.

Очевидно, що такі потужні технічні можливості через потенційно небезпечне інтернет-з'єднання необхідно надійно захистити від можливих атак. Насправді безпека – це пріоритетний напрямок нашого розвитку й головний фактор, яким ми керуємося під час розробки програмного забезпечення. Ми хочемо гарантувати безпечний доступ до вашого комп'ютера й захистити власні інтереси: мільйони користувачів по всьому світу довіряють лише безпечним рішенням, і лише вони гарантують стабільний успіх у веденні бізнесу.

Оцінювання незалежних експертів

Наше програмне забезпечення TeamViewer відзначено п'ятизірковим знаком якості (найвища винагорода) Федеральної асоціації IT-експертів і консультантів (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). Незалежні експерти BISG e.V. перевіряють продукцію кваліфікованих виробників щодо якості, безпеки й робочих характеристик.

Рекомендації

Зараз програму TeamViewer використовують понад 200 млн користувачів. Найвідоміші міжнародні корпорації з усіх сфер діяльності (зокрема особливо секретних, як-от банківські установи, заклади фінансування, охорони здоров'я, а також урядові організації) успішно використовують TeamViewer.

Ми пропонуємо вам переглянути відгуки про нашу програму, які легко можна знайти в Інтернеті, щоб скласти перше враження про прийнятність нашого рішення. Ви дізнаєтеся, що більшість компаній, які мали схожі вимоги до безпеки й доступності програмного забезпечення, після ретельної перевірки вибрали TeamViewer. Однак, щоб ви змогли скласти власне перше враження, перегляньте технічні характеристики, зазначені в решті документації.

Сеанси TeamViewer

Створення сеансу та типи підключень

На початку створення сеансу програма TeamViewer визначає оптимальний тип підключення. Після синхронізації з головними серверами в 70% випадків установлюється пряме підключення через протоколи UDP або TCP (навіть після підключення стандартних шлюзів, механізмів NAT і брандмауерів). Решта підключень здійснюється через нашу резервну мережу маршрутизаторів через протокол TCP або тунелі http. Для роботи з TeamViewer не потрібно відкривати жодні порти

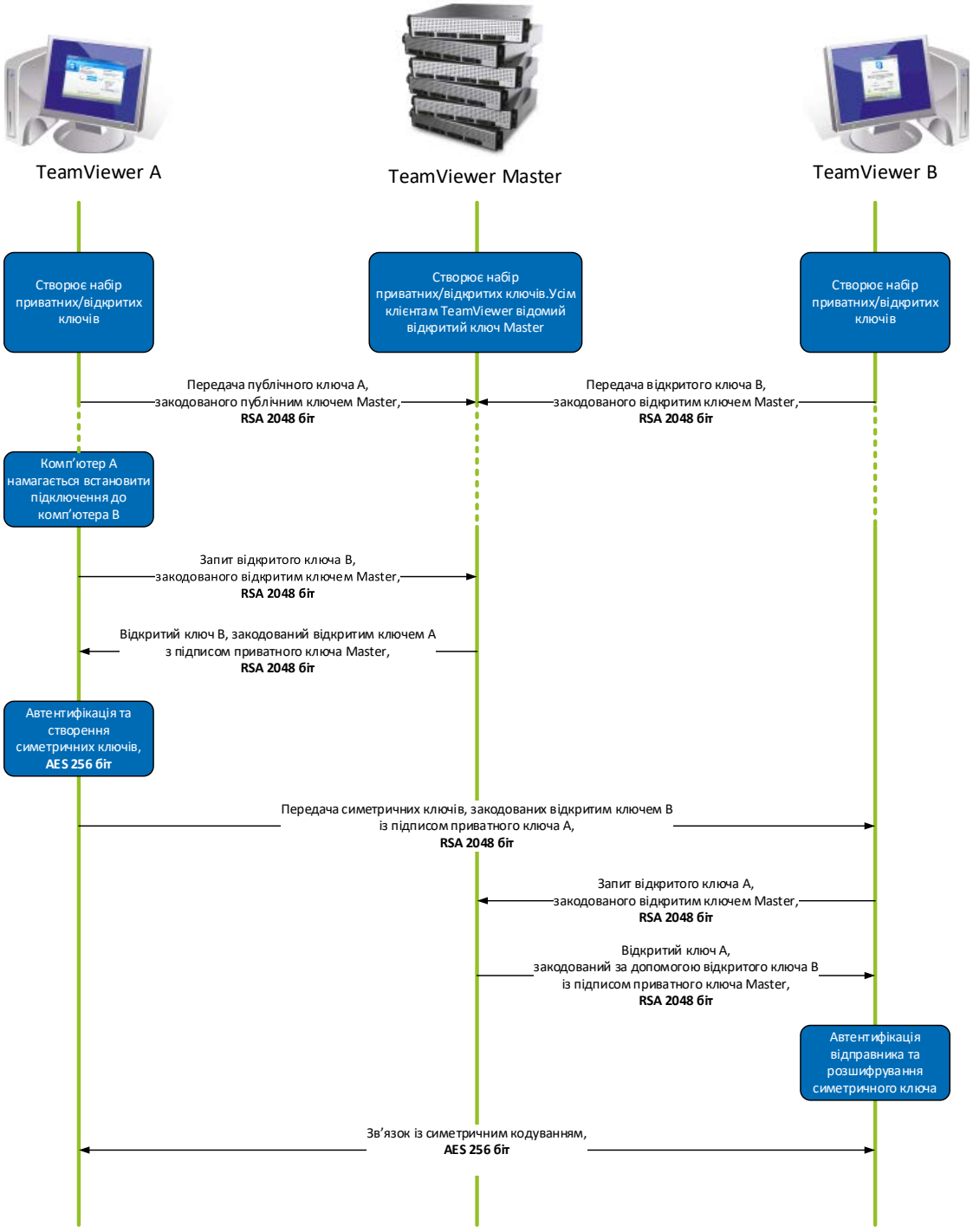
Як зазначено в наведеному нижче розділі «Шифрування й автентифікація», навіть ми, оператори серверів маршрутизації, не можемо читати зашифрований трафік даних.

Шифрування й автентифікація

Трафік програми TeamViewer захищено за допомогою алгоритму обміну відкритими/індивідуальними ключами RSA та алгоритму шифрування сеансу AES (256 біт). Ця технологія використовується в порівнянній формі для http/SSL і згідно із сучасними стандартами вважається абсолютно безпечною. Оскільки індивідуальний ключ ніколи не залишається на комп'ютері клієнта, ця процедура забезпечує неможливість розшифрування потоку даних з'єднаними комп'ютерами, зокрема серверами маршрутизації TeamViewer.

Кожний клієнт TeamViewer, що вже встановив відкритий ключ головного кластера, може розшифровувати повідомлення до головного кластера та перевіряти повідомлення від нього. PKI (інфраструктура відкритих ключів) ефективно запобігає атакам через посередника. Незважаючи на шифрування, пароль ніколи не надсилається напряму – тільки через процедуру «запит-відповідь» і зберігається лише на локальному комп'ютері.

У процесі автентифікації пароль ніколи не передається напряму, оскільки використовується протокол SRP. На локальному комп'ютері зберігається лише засіб перевірки пароля.



Шифрування й автентифікація TeamViewer

Перевірка ідентифікаторів TeamViewer

Ідентифікатори TeamViewer автоматично створюються в програмі на основі різних характеристик апаратного й програмного забезпечення. Перед підключенням сервери TeamViewer перевіряють дійсність цих ідентифікаторів.

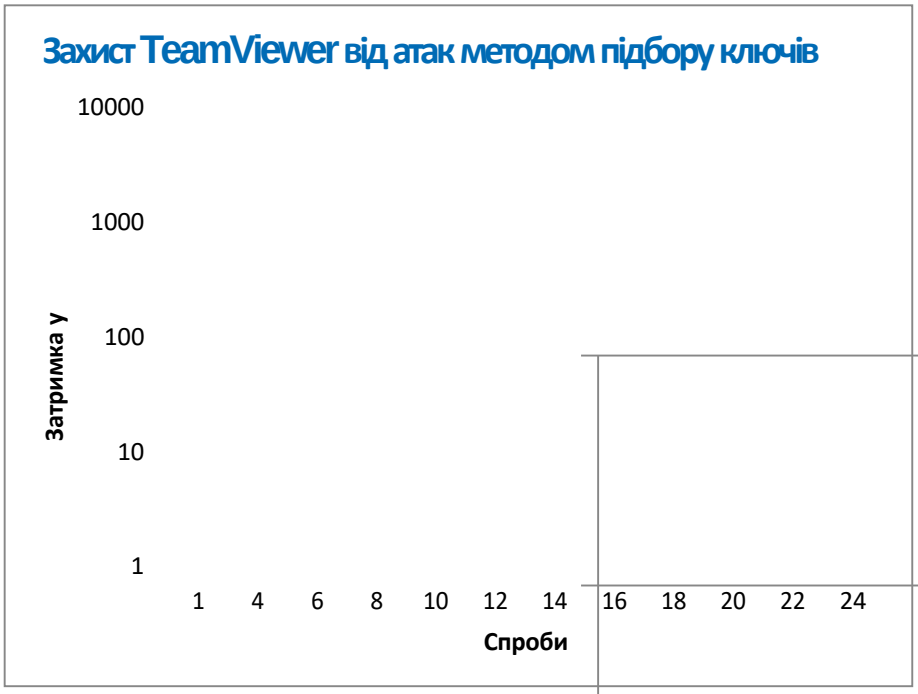
Прямий захист

Потенційні клієнти, які цікавляться безпекою TeamViewer, постійно запитують про шифрування. Очевидно, найбільше користувачі бояться того, що третя сторона може відстежувати підключення або перехопити дані доступу до програми TeamViewer. Однак насправді найнебезпечнішими частіше бувають примітивні атаки.

У контексті комп'ютерної безпеки «прямі атаки» – це метод спроб і помилок для вгадування пароля, який захищає ресурс. Завдяки потужності стандартних комп'ютерів, яка постійно збільшується, час, необхідний для вгадування довгих паролів, значно скорочується.

З метою захисту від прямих атак програма TeamViewer суттєво збільшила затримку між спробами підключення. Таким чином, для 24 спроб потребуватиметься 17 годин. Затримку буде скасовано лише після успішного введення пароля.

Програма TeamViewer оснащена не лише механізмом захисту клієнтів від атак з одного певного комп'ютера, але також із багатьох комп'ютерів, що становлять бот-мережу й використовуються для того, щоб отримати доступ до одного конкретного ідентифікатора TeamViewer.



Графік: Час, що минає після N кількості спроб, ужитих під час прямої атаки

Підписування коду

Для додаткового захисту все наше програмне забезпечення підписується через сертифікат VeriSign Code Signing. Таким чином, завжди можна визначити видавця програмного забезпечення. Якщо програмне забезпечення згодом змінюється, цифровий підпис автоматично стає недійсним.

Центри обробки даних і магістральна мережа передачі інформації

Щоб гарантувати найвищу безпеку й доступність послуг програми, усі сервери TeamViewer розташовуються в центрах обробки даних, які відповідають стандарту ISO 27001 і використовують велику кількість з'єднань та резервних джерел живлення. Для цього застосовується лише ультрасучасне фірмове апаратне забезпечення. Усі сервери, на яких міститься конфіденційна інформація, розташовані в Німеччині або Австрії.

Відповідність стандарту ISO 27001 означає, що персональний контроль доступу, відеоспостереження, датчики руху, цілодобове щоденне спостереження й охорона об'єкта надають доступ до центрів обробки даних лише вповноваженим особам і гарантують найкращий захист даних та апаратного забезпечення. На єдиному пункті пропуску в центр обробки даних здійснюється ретельна перевірка ідентифікації особистості.

Обліковий запис TeamViewer

Облікові записи TeamViewer розміщуються на спеціальних серверах TeamViewer. Щоб отримати інформацію щодо керування доступом, перегляньте наведений вище розділ «Центри обробки даних і магістральна мережа передачі інформації». Для авторизації й шифрування пароля використовується протокол парольної автентифікації SRP – розширений протокол на основі методу PAKE (вироблення загального ключа з автентифікацією на основі пароля). У випадку здійснення прямої атаки або атаки через посередника неможливо отримати достатню кількість даних для підбору пароля. Це означає, що, навіть за умови використання слабких паролів, застосовуватиметься надійна система захисту. Конфіденційні дані в обліковому записі TeamViewer, як-от облікові дані для входу в хмарне сховище, зберігаються в стандартах шифрування AES/RSA 2048 біт.

Консоль керування

Консоль керування TeamViewer – це веб-платформа для керування користувачами, створення звітів про з'єднання й керування комп'ютерами та контактами. Вона знаходиться в центрах обробки даних, що відповідають стандарту ISO 27001 і HIPAA. Усі дані передаються через безпечний канал за допомогою протоколу шифрування TSL (захист на транспортному рівні), що є стандартом для безпечного інтернет-з'єднання. Крім того, конфіденційні дані зберігаються в зашифрованому вигляді згідно зі стандартами шифрування AES/RSA 2048 біт. Для авторизації й шифрування пароля використовується протокол SRP. SRP – це перевірений надійний безпечний метод автентифікації на основі пароля й обміну ключами за допомогою модуля 2048 біт.

Налаштування на основі правил

З консолі керування TeamViewer користувачі можуть визначати, розповсюджувати й упроваджувати правила налаштувань для програмного забезпечення TeamViewer на пристроях, що належать їм особисто. Правила налаштувань мають цифровий підпис облікового запису, за допомогою якого вони створюються. Таким чином, лише одному обліковому запису дозволяється призначати політику пристрою, який за ним закріплений.

Програмна безпека в TeamViewer

Чорний і білий списки

Якщо TeamViewer використовується для підтримки автономних комп'ютерів (тобто TeamViewer інсталюється як служба Windows), деяких клієнтів може зацікавити додатковий параметр безпеки для обмеження доступу до цих комп'ютерів.

За допомогою білого списку можна чітко вказати, які ідентифікатори та/або облікові записи TeamViewer можуть мати доступ до комп'ютера. Використовуючи чорний список, можна заблокувати певні ідентифікатори й облікові записи TeamViewer. Центральний білий список доступний як частина налаштувань на основі політики, описаних у наведеному вище розділі «Консоль керування».

Шифрування чатів і відео

Історії чатів, пов'язаних з обліковим записом TeamViewer, зашифровані й зберігаються відповідно до тих самих стандартів AES/RSA 2048 біт, як описано в розділі «Обліковий запис TeamViewer» Усі повідомлення чату й відеотрафік повністю шифруються протягом сеансу за допомогою алгоритму AES (256 біт).

Відсутність режиму непомітності

Не існує функції, яка дасть змогу використовувати TeamViewer у фоновому режимі. Навіть якщо програма запущена як служба Windows у фоновому режимі, її роботу завжди буде видно за допомогою значка на панелі сповіщень.

Після встановлення підключення над панеллю сповіщень постійно відображатиметься невелика панель керування. Через це TeamViewer не підходить для навмисного прихованого спостереження за діяльністю на комп'ютері або контролем роботи працівників.

Захист пароля

Для надання клієнту термінової підтримки TeamViewer (TeamViewer QuickSupport) створює пароль сеансу (одноразовий пароль). Ви можете підключитися до комп'ютера клієнта, указавши ідентифікатор і пароль, який він назве. Після повторного запуску програми TeamViewer на комп'ютері клієнта буде створено новий пароль сеансу, тож до його комп'ютера можна підключатися, лише коли вас попросять це зробити.

Щоб запускати TeamViewer для віддаленої підтримки автономних пристроїв (наприклад, серверів), потрібно встановити індивідуальний постійний пароль, який забезпечить постійний вхід на цей комп'ютер.

Керування вхідним і вихідним доступом

Ви можете окремо налаштовувати режими підключення програми TeamViewer. Наприклад, можна налаштувати віддалену підтримку комп'ютера без необхідності входу в його систему.

Обмеження функціональних можливостей цих функцій насправді необхідні завжди, оскільки вони допомагають скоротити кількість можливих уразливих місць для потенційних атак.

Двофакторна автентифікація

Програма TeamViewer допомагає компаніям, що використовують стандарт HIPAA і шину PCI. Двофакторна автентифікація додає ще один рівень безпеки для захисту облікових записів

Щоб пройти автентифікацію, крім імені користувача й пароля необхідно ввести код. Він генерується через алгоритм створення тимчасових одноразових паролів (TOTP). Тому код дійсний лише протягом короткого періоду часу.

Завдяки двофакторній автентифікації й обмеженню доступу за допомогою створення білого списку програма TeamViewer допомагає відповідати всім необхідним критеріям для сертифікації HIPAA і PCI.

Тестування безпеки

Інфраструктура й програмне забезпечення TeamViewer підлягають ретельній регулярній перевірці. Перевірки виконуються незалежними компаніями, які спеціалізуються на тестуванні безпеки.

Залишилися запитання?

Щоб поставити запитання або отримати додаткову інформацію, звертайтеся за телефонами +380 443609564 або надсилайте листи на адресу support@teamviewer.com.

Контактні дані

TeamViewer GmbH
Jahnstr. 30
D-73037 Göppingen
Німеччина