

Здравствуйтесь, Ignacio Otegui



17 и 18 октября злоумышленники получили доступ к части нашей инфраструктуры через уязвимость в системе управления виртуализацией VMmanager 6, которая используется нами для управления инфраструктурой виртуализации. Проблема связана исключительно с халатностью разработчиков VMmanager 6 - ispsystem

Внимание! Если Ваша услуга была создана 18 октября 2026 года и позднее - Вас инцидент не касается.

Что произошло:

Злоумышленники запустили на части серверов нашей инфраструктуры виртуализации программу для кражи данных. Она подключала диски клиентских виртуальных серверов в режиме только для чтения и копировала с них:
- пароли, ключи доступа (SSH, API, облачные сервисы) и токены:

Hola, Ignacio Otegui



Los días 17 y 18 de octubre, unos atacantes accedieron a parte de nuestra infraestructura a través de una vulnerabilidad en el sistema de gestión de virtualización VMmanager 6, que utilizamos para administrar nuestra infraestructura virtualizada. El problema se debe exclusivamente a la negligencia de los desarrolladores de VMmanager 6: ispsystem.

¡Atención! Si su servicio se creó el 18 de octubre de 2026 o después, este incidente no le afecta.

¿Qué sucedió?

Los atacantes lanzaron malware de robo de datos en algunos servidores de nuestra infraestructura virtualizada. Montaron los discos de los servidores virtuales de los clientes en modo de solo lectura y copiaron lo siguiente:
- contraseñas, claves de acceso (SSH, API, servicios en la nube) y tokens;

- конфигурационные файлы и историю команд;
- криптокошельки;
- пользовательские файлы.

Собранные данные отправлялись на сервер злоумышленников.

К сожалению, Ваш сервер s219564.hostiman.com затронут данной проблемой.

Атака затронула не всю инфраструктуру, а только часть узлов виртуализации.

Пострадали клиентские серверы, которые на них работали.

Программа ничего не

меняла на дисках виртуальных серверов и не запускалась

внутри них. Поэтому на

самом сервере следов атаки нет, и он работает как обычно.

Если вы получили

уведомление в личном кабинете, считайте, что данные с

сервера были скопированы.

Данные наших клиентов, персональные данные и прочая

информация, не была

затронута. Инцидент не касается биллинга HostiMan, утечки с

серверов под

- archivos de configuración e historial de comandos;

- monederos de criptomonedas;

- archivos de usuario.

Los datos recopilados se enviaron al servidor de los atacantes.

Lamentablemente, su servidor s219564.hostiman.com se ha visto afectado por este problema.

El ataque no afectó a toda la infraestructura, sino solo a algunos nodos de virtualización.

Los servidores cliente afectados se ejecutaban en dichos nodos. El programa no modificó nada en los discos del servidor virtual ni se ejecutó dentro de ellos. Por lo tanto, no hay rastros del ataque en el servidor, que funciona con normalidad. Si recibió una notificación en su cuenta personal, tenga en cuenta que se copiaron los datos del servidor.

Los datos de nuestros clientes, los datos personales y demás información no se vieron afectados. El incidente no afecta a la facturación de HostiMan: no se produjeron fugas de datos en los

данные наших клиентов, персональные данные и прочая информация, не была затронута. Инцидент не касается биллинга HostiMan, утечки с серверов под управлением HostiMan не производилось. Затронуты только клиентские сервера VDS на большинстве узлов виртуализации.

Что уже сделали:

Сразу после обнаружения атаки мы отключили внешний доступ к системе управления виртуализацией, через которую она была проведена. Именно это сейчас защищает инфраструктуру от повторной атаки тем же способом. Мы также заблокировали в нашей сети адрес сервера злоумышленников. Работа VMmanager 6 ограничена с нашей стороны.

На текущий момент вендор выпустил промежуточный патч и работает над окончательным исправлением, мы на связи с ним. Пока уязвимость не будет

Los datos de nuestros clientes, los datos personales y demás información no se vieron afectados. El incidente no afecta a la facturación de HostiMan; no se produjeron fugas de datos en los servidores gestionados por HostiMan. Solo se vieron afectados los servidores VDS de los clientes en la mayoría de los nodos de virtualización.

Acciones ya tomadas:

Inmediatamente después de detectar el ataque, deshabilitamos el acceso externo al sistema de gestión de virtualización a través del cual se llevó a cabo. Esto protege ahora la infraestructura de un posible ataque repetido con el mismo método. También hemos bloqueado la dirección del servidor del atacante en nuestra red. El funcionamiento de VMmanager 6 está restringido en nuestro sistema.

El proveedor ha publicado un parche provisional y está trabajando en la solución definitiva; estamos en contacto con él. Hasta que la vulnerabilidad se corrija por completo, el acceso al sistema permanecerá bloqueado.

¿Qué debe hacer?

уязвимость не будет
полностью устранена, доступ к системе останется закрытым.

Что нужно сделать вам?

Главный риск — в том, что злоумышленники воспользуются украденными паролями и ключами. Поэтому важно сменить их как можно скорее.

1. Криптокошельки: в первую очередь переведите средства на новые кошельки, созданные на другом, чистом устройстве.
2. Пароли и ключи: смените все пароли, SSH-ключи, API-ключи и токены, которые хранились на сервере: root и пользователей, базы данных, панели управления сайтами, почту, облачные сервисы, CI/CD, платёжные системы.
3. Отзовите старые ключи, а не просто создайте новые: в облачных консолях, GitHub/GitLab, у платёжных провайдеров.
4. Проверьте журналы входов на самом сервере и в сервисах, ключи от которых на нём лежали: не было ли входов с незнакомых адресов после 17

¿Qué debe hacer?

El principal riesgo es que los atacantes utilicen contraseñas y claves robadas. Por lo tanto, es importante cambiarlas cuanto antes.

1. Carteras de criptomonedas: Primero, transfiera los fondos a nuevas carteras creadas en un dispositivo diferente y limpio.
2. Contraseñas y claves: Cambie todas las contraseñas, claves SSH, claves API y tokens almacenados en el servidor: root y usuarios, bases de datos, paneles de control del sitio web, correo electrónico, servicios en la nube, CI/CD y sistemas de pago.
3. Revoque las claves antiguas; no cree nuevas: en consolas en la nube, GitHub/GitLab o con proveedores de pago.
4. Revise los registros de inicio de sesión del servidor y de los servicios donde se almacenaron las claves: no se registraron inicios de sesión desde direcciones desconocidas después del 17 de octubre. Si el atacante logró iniciar sesión antes del cambio de contraseña, revise `~/.ssh/authorized_keys`, los nuevos usuarios, las tareas programadas (cron jobs) y los servicios systemd.
5. Si los datos personales de sus clientes se encontraban en el servidor, consulte con un abogado sobre la obligación de notificar a

4. Проверьте журналы входов на самом сервере и в сервисах, ключи от которых на нём лежали: не было ли входов с незнакомых адресов после 17 октября. Если злоумышленник успел войти до смены паролей, проверьте ~/.ssh/authorized_keys, новых пользователей, задания cron и службы systemd.

5. Если на сервере были персональные данные ваших клиентов, проконсультируйтесь с юристом об обязанности уведомить Роскомнадзор.

Вы можете написать в поддержку, мы сможем помочь изменением паролей, перенастройкой сайтов, но просим учитывать, что срок решения проблем будет увеличен в связи с нагрузкой на поддержку - рекомендуем меры оперативно принимать своими силами.

С уважением, Ваш хостинг-провайдер HostiMan.

Zdravstvuyte, Ignacio Otegui 17 i 18 oktyabrya zloumyshlenniki poluchili dostup k chasti nashey infrastruktury cherez uyazvimost' v sisteme upravleniya virtualizatsiyey VMmanager 6, kotoraya ispol'zuyetsya nami dlya upravleniya infrastrukturoy

[Show more](#)

tareas programadas (cron jobs) y los servicios systemd.

5. Si los datos personales de sus clientes se encontraban en el servidor, consulte con un abogado sobre la obligación de notificar a Roskomnadzor.

Puede contactar con soporte técnico; podemos ayudarle con cambios de contraseña y reconfiguraciones del sitio web, pero tenga en cuenta que el tiempo de resolución de estos problemas se prolongará debido a la carga de trabajo de nuestro equipo de soporte. Le recomendamos que tome medidas inmediatas.

Atentamente, Su proveedor de hosting, HostiMan.