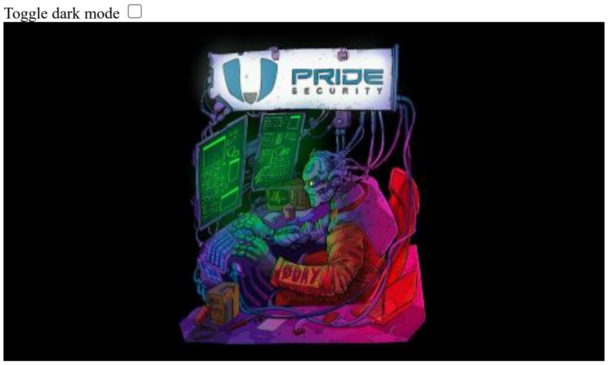
Multiple security vulnerabilities affect…

2 years ago

Tags

- CVE
- Hacking
- PAX STORE
- PAX TECHNOLOGY
- Pride Security
- PrideSec
- Security Advisory

Toggle dark mode □



Multiple security vulnerabilities affect PAXSTORE (PAX Technology) - PSADV2021-001

May 14, 2021 • Altere o idioma para BR

□

Disclaimer
This Security Advisory is provided on an "as is" basis and do not imply any kind of guarantee or warranty. Your use of the information in this publication or linked materials is at your own risk. PRIDE Security reserves the right to change or update this content without notice at any time.

About manufacturer
PAX Technology, founded in 2001, is one of the world leaders in payment terminals. PAX has delivered over 45 million terminals to more than 120 countries around the world. Packed with the latest technology and internationally required security certifications.
Site: https://marketing.paxtechnology.com/about-pax

About the product
PAXSTORE is a product of PAX Technology connecting over 1 million terminals, thousands of app developers, and more than 150 marketplaces in over 80 countries worldwide.

You can have your own independent marketplace in minutes. Full lifecycle POS apps management functionalities are ready for your using. You can create an out-of-the-box tailored apps solution based on the category of merchant and specific needs they require.

As the owner of a smart POS terminal, or if are an organization that manages a large number of such devices, you will have full management and monitoring capabilities and can perform real-time operations for the deployed terminals through PAXSTORE.

Rich payment industry value-added services, so that you can easily manage your terminals, apps and merchants. Business Intelligent will be your close assistant to do business strategy.
Site: https://www.whatspos.com/

Versions affected
PAXSTORE version 7.5 and lower (PAX Technology)

Summary
In July 2020, PRIDE Security was hired to assess the security of software and hardware in PAX Technology's products purchased by one of their customers. In December 2020, after the contractor mitigated the security issues found in its environment, PAX Technology was communicated about some of the software security vulnerabilities relevant to the PAXSTORE ecosystem.

These security issues discovered in the PAXSTORE marketplace's APIs show a high security risk, since these vulnerabilities could compromise the entire environment when properly exploited by an attacker. In general, these vulnerabilities allow privilege escalation (horizontal and vertical), in addition permits to list and to read files from the Web server.

PRIDE Security is reporting these vulnerabilities with the purpose to awareness about the risks in PAXSTORE ecosystem, as well encouraging customers to immediate update to the latest version (8.0).

Impact
To illustrate the impact, during this engagement PRIDE Security abused this security issues to compromise the private keys of JWT token used by the marketplace analyzed and reused them to manipulate the access tokens to access the platform as any desired user (clients and administrators). Thereafter, an attacker could easily force the remote installation of any application in thousands of payment terminals managed by PAXSTORE.

It is worth mentioning that this technique could be used for several purposes, such as the creation of botnets aimed to launch Distributed Denial of Service (DDoS), theft financial information, force all payment terminals managed through the platform to stay in non-operating state (off-line), fraud, etc.

Based on the security issues identified in the PAXSTORE ecosystem, it is estimated that more than 150 PAXSTORE marketplaces in the world are currently vulnerable, and the lack of diligence can put millions of payment terminals at risk and cause immeasurable damage.

Finding 1: XML External Entity – XXE (CVE-2020-36124)

The PAXSTORE ecosystem allows that anyone sign-up as a developer at marketplace (https://paxstore-marketpace-customer.com/developer). As describe in the PAXSTORE documentation, the developer can define an XML template for its application.

However, two of those endpoints available in that panel, are vulnerable to XXE. They are:

- POST /p-market-web/v1/developers/apks/{App-ID}/paramTemplateSchema;
- POST /p-market-web/v1/developers/{Dev-ID}/app/{App-ID}/paramAnalysis.

Example - HTTPS Request (shortened):

```
POST /p-market-web/v1/developers/apks/{APK-ID}/paramTemplateSchema HTTP/1.1
Host: api.a-paxstore-marketplace-domain.com
Authorization: Bearer Developer-Access-Token
X-Market-Domain: X-Market-Domain-Name
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarykVegzdE7IoasleA2

------WebKitFormBoundarykVegzdE7IoasleA2
Content-Disposition: form-data; name="paramTemplateFile"; filename="PrideSec.xml"
Content-Type: text/xml

<!DOCTYPE foo [<!ENTITY load SYSTEM "file:///path/to/conf/fs.properties" >]>
<Schema>
<Groups>
<Group>
<ID>sys_G0</ID>
<Title>&load;</Title>
…
</Group>
</Groups>
…
</Schema>------WebKitFormBoundarykVegzdE7IoasleA2
Content-Disposition: form-data; name="paramTemplateName"

undefined
------WebKitFormBoundarykVegzdE7IoasleA2--
```

Example - HTTPS Response (shortened):

```
HTTP/1.1 200
Content-Type: application/json;charset=UTF-8

{"paramTemplateName":"paramTemplateFile","groupList":[{"id":"","title":"XXE-RETURN-HERE”…}]}]}]}
```

The *XML External Entity* injection (as known as XXE) is a security issue that allows an attacker to manipulate the processing of XML data. In this case, it allows the attacker to list and read files from the APIs server. Among the files accessible on the back-end, was possible to identify that the /path/to/conf/fs.properties contains sensitive information, such as signing keys.

Finding 2: Insecure direct object references – IDOR (CVE-2020-36126)

PAXSTORE marketplace’s endpoints allows an authenticated user to read and write data not owned by them, including data from third-party users, application and payment terminals.

This behavior represents a *Broken Access Control – IDOR* vulnerability. In total, 26 endpoints were identified with this class of vulnerability.
As described, this kind of vulnerability allows an attacker to impersonate any user, may lead to the unauthorized disclosure, modification or destruction of its information.

The following endpoints are vulnerable with *IDOR*:

- GET /p-market-web/v1/developers/apps/{App-ID}
  It allows a developer to collect information about any application from marketplace, for example, the App Key and App Secret, given the App ID (sequential value starting from 1000000001).

- PUT /p-market-web/v1/developers/apps/{App-ID}/appKey
  It allows a developer to update sensitive information, as App Key and App Secret of any applications in the marketplace, given the AppID (sequential value starting from 1000000001).

- GET /p-market-web/v1/terminals/{Terminal-ID}/installedApks
  It allows an user without administrative privileges to list installed application in any payment terminal, given the Terminal ID (value with 10 numerical digits starting from "1000").

- DELETE /p-market-web/v1/users/notification/messages/{Message-ID}
  It allows an user without administrative privileges to delete received message of other users, given the Message ID (value of 10 numerical digits starting from “1000”).

- PUT /p-market-web/v1/developers/sandbox/terminals/{Sandbox-Terminal-ID}
  It allows a developer to add sandbox terminals in other user’s accounts, given the Sandbox Terminal ID (sequential value starting from 1).

- GET /p-market-web/v1/developers/sandbox/terminals/{Sandbox-Terminal-ID}
  It allows a developer to collect information about sandbox terminals of other users, given Sandbox Terminal ID (sequential value starting from 1).

- DELETE /p-market-web/v1/developers/sandbox/terminals/{Sandbox-Terminal-ID}
  It allows a developer to delete sandbox terminal of other user’s accounts, given the Sandbox Terminal ID (sequential value starting from 1).

- GET /p-market-web/v1/terminals/serialNo/{Terminal-SerialNo}
  It allows an user without administrative privileges to collect information of any payment terminal, given the serial number (value with 10 numerical digits, usually starting from “117”).

- GET /p-market-web/v1/users/{User-ID}
  It allows a developer or reseller to collect user’s profile information (name, e-mail, phone number, login name, account privilege, last login timestamp, etc.), given the User ID (sequential value starting from 1000000001).

- POST /p-market-web/v1/developers/enterprise/{User-ID}/admin?admin=true
  It allows a developer to change the status Developer Admin (true or false) of any user’s accounts, given the victim User ID (sequential value starting from 1000000001).

- POST /p-market-web/v1/feedbacks
  It allows an user without administrative privileges to create feedback messages, with a crafted ID of any payment terminal in the payload, that can induce other users to believe that this message was created by the terminal owner.

- DELETE /p-market-web/v1/feedbacks/{Feedback-ID}
  It allows an user without administrative privileges to remove feedback messages, given its ID (sequential value starting from 1).

- POST /p-market-web/v1/developers/apks/{Apk-ID}/originFile
  It allows an user without administrative privileges to download (downloadTaskId) any Android application available at Store without platform signature, even those that are restrict for a specific resellers group. For that, an attacker must include the Apk-ID (sequential value starting from 1000000001).

- DELETE /p-market-web/v1/developers/apps/{App-ID}
  It allows a developer to delete application available in the marketplace, given the App ID (sequential value starting from 1000000001). Once done, it is impossible to restore the application deleted.

- POST /p-market-web/v1/developers/apps/{App-ID}/apks/file
  It allows a developer to add an APK in any application project, given the App ID (sequential value starting from 1000000001).

- POST /p-market-web/v1/developers/apps/{App-ID}/apks/{Apk-ID}/file
  It allows a developer to add a new APK version for any application in the marketplace, given the App ID and Apk ID.

- DELETE /p-market-web/v1/developers/apps/{App-ID}/apks/{Apk-ID}
  It allows a developer to remove a specific APK version of any application in the marketplace, given the App ID and ApkID.

- POST /p-market-web/v1/developers/apps/{App-ID}/apks/{Apk-ID}/submit
  It allows a developer to submit a new APK version to be approved for any application in the marketplace (even the ones not authorized to this developer), given App ID and Apk ID. If the administrator approves, the application will be available for download in the platform.

- POST /p-market-web/v1/admin/apps/{App-ID}/specific
  It allows a reseller to distribute any application in the marketplace (even the not available to this reseller) to their own POS terminals. With that, a reseller can access application distributed by other resellers.

- GET /p-market-web/v1/admin/apps/{App-Id}/installed/terminals
  It allows a reseller to verify which terminals downloaded a particular application, even for apps that they do not own.

- POST /p-market-web/v1/admin/apps/apks/{Apk-ID}/file
  It allows a reseller to download of any application from the marketplace, even those that they do not own.

- GET /p-market-web/v1/terminals/{Terminal-ID}/configurations
  It allows a reseller the access some hardware status of any payment terminal (ex.: GPS status, screen brightness, language, POS volume).

- GET /p-market-web/v1/terminals/{Terminal-ID}/installedFirmware
  It allows a reseller to access the firmware name installed in the POS terminal.

- GET /p-market-web/v1/admin/apps
  It allows a reseller to get a list of available applications in the marketplace, even those that they do not own.

- GET /p-market-web/v1/guides/admin/docs/{Doc-ID}
  It allows an user without administrative privileges to access documentation of the administrator panel guide, given the Doc-ID (sequential value starting from 1).

- GET /p-market-web/v1/guides/super/docs/{Doc-ID}
  It allows an user without administrative privileges to access the documentation of the global administration panel guide, given the Doc-ID (sequential value starting from 1).

Finding 3: Obtaining a signing certificate and its password (CVE-2020-36127)

PAXSTORE marketplace gives users with administrator privilege control over extra platform features, such as the public certificate key responsible for signing Android applications at payment terminals.

Opening the marketplace administration panel and accessing the PUK Signature functionality, the administrator will not have access to the current p12 certificate and password. That occurs due the Web application request the endpoint GET /p-market-web/v1/admin/signature.

When accessing this functionality, the user has the option to replace the current certificate through the interface and it is not possible to view the certificate password (p12) already deployed on the platform. However, an endpoint was identified, not accessible through the administrative interface, which returns the p12 certificate in base64 with its password, and both can be accessed even by users with reseller privilege.

The mentioned endpoint is:

- GET /p-market-web/v1/admin/signature/signaturePuk
  Returns the current p12 certificate in base64 with its password.

Example - HTTPS Request (shortened):

```
GET /p-market-web/v1/admin/signature/signaturePuk HTTP/1.1
Host: api.a-paxstore-marketplace-domain.com
Authorization: Access-Token-from-Reseller-or-greater-privilege
X-Market-Domain: X-Market-Domain-Name
```

Example - HTTPS Response (shortened):

```
HTTP/1.1 200
Content-Type: application/json;charset=UTF-8

{…"password":"PASSWORD-RETURNED-HERE","certificateName":"CERTIFICATE-NAME-RETURNED-HERE","certificate":"CERTIFICATE-RETURNED-HERE"…}
```

Finding 4: X-Terminal-Token can be retried without a password (CVE-2020-36128)

A payment terminal that has the marketplace application installed on its operating system allows the user to download the available applications.

Each payment terminal has a session token (called X-Terminal-Token) to access the marketplace. This allows the store to identify the terminal and make available the applications distributed by its reseller. In addition, all remote communication with the marketplace, which includes sending commands, changing hardware status (among others), is done based on the X-Terminal-Token token present in the terminal.

However, during the process to intercept HTTPS traffic from the application store, it was possible to collect the request responsible for assigning the X-Terminal-Token to the terminal and there is no password or security key that prevents the terminal from obtaining a X-Terminal-Token crafted pretending to be another device.

The mentioned endpoint is:

- POST /p-market-api/v1/terminal/login

An attacker can use this behavior to authenticate its own payment terminal in the application store impersonating another device.

For example, this will allow a terminal to no longer be managed by its real reseller, or even to have access to other restricted applications.

Finding 5: Password revalidation in sensitive operations can be bypassed (CVE-2020-36125)

The PAXSTORE marketplace gives users with administrator privilege the control over sensitive operations, like upload of a new certificate signature of Android application.

Every time that actions is requested, is necessary that user to enter its password again, even if the administrator is already authenticated. However, this password validation can be easily bypassed by requesting the endpoint directly. Thus, in a scenario where an attacker has access to a user's session, all types of action can be taken, even without the consent of the person responsible.

However, this validation, although performed on the backend, does not prevent the user from requesting the operation directly, for example, through the endpoint below.

- GET /p-market-web/v1/admin/signature

Password revalidation is also required when trying to view the Access Secret of the credential belonging to integration with external systems. Also, when the authenticated user's password is unknown, it is possible to directly request the endpoint below, responsible for returning the Access Secret.

- GET /p-market-web/v1/admin/market/3rdsys/config/secret

Note that the credential of external systems provides access to several sensitive application endpoints. To use them, just follow the steps of the PAXSTORE Open API project, available at GitHub (https://github.com/PAXSTORE/paxstore-openapi-java-sdk). Therefore, its exposure represents a relevant risk to applications.

Vulnerabilities recommendation
PAX Technology released version 8.0 where they informed PRIDE Security that all the security issued above were fixed.

It's important to note that PRIDE Security did not retested or confirmed that the fixes are effective.

Communication timeline with manufacturer
• December 02, 2020 – Contact over e-mail (attempt 1).
• December 30, 2020 – Contact over e-mail (attempt 2).
• December 31, 2020 – PAX Technology acknowledge receipt of the email.
• January 07, 2021 – PAX Technology provides a roadmap to fix all issues.
• April 25, 2021 – PAX Technology released version. 8.0 with fixes.
• May 14, 2021 – Public release (PRIDE Security).

Acknowledgements

Name	Company
Ricardo B. Gonçales	PRIDE Security
Andriel C. S. Biagioni	PRIDE Security

About PRIDE Security
PRIDE Security is a company specialized in information security that focuses on technical excellence and personalized services. Founded by information security experts, we have worked in various types of projects, from ATM (automated teller machines) penetration testing to national security projects.

Composed of an experienced team of more than 15 years in the market and with technical excellence proven by national and international technical recognition, PRIDE Security sees in each project a new challenge to deliver more than expected.

As proof of international technical recognition, our professionals are constantly approved or invited to lecture on security events around the world. We cite below some examples of congresses, conferences and seminars focused on information security, which we participate as lecturers or coordinators of the technical groups:

• Blackhat – USA
• RSA Conference – USA
• Defcon – USA
• ToorCon – USA
• Blackhat – Europe edition
• OWASP AppSec Research – Europe edition
• OWASP AppSecEU09 – Europe edition
• Troppers – Germany
• H2HC (Hackers 2 Hackers Conference) – Brazil
• YSTS (You Sh0t The Sheriff) – Brazil

In addition to lecturing at major security events around the world, our team of experts are also responsible for writing various papers, co-author of offensive technology patent registered in the United States of America (US8756697), finding and publishing security vulnerabilities in famous software such as Sun Solaris, FreeBSD / NetBSD kernel, QNX RTOS, Microsoft ISA Server, Microsoft Word, Adobe Flash, Adobe PDF, among others.

Many organizations of all sizes concerned with information security rely on PRIDE Security. If you aim, we will be pleased to connect you with our customers to share about their experience with our services.

Tags

- Pride Security
- PrideSec
- Security Advisory
- Hacking
- PAX TECHNOLOGY
- PAX STORE
- CVE

Subscribe to our newsletter

Get the latest posts delivered right to your inbox.

Your email address Your email address
Subscribe

Now check your inbox and click the link to confirm your subscription.

Please enter a valid email address

Oops! There was an error sending the email, please try later.

PRIDE Security

Among with Ricardo Bernardini

PRIDE Security is a consultancy specialized in information security that offers customized services and products to meet every business' needs and goals.

-

Recommended for you

No posts found

Apparently there are no posts at the moment, check again
later.

Ótimo! Você se inscreveu com sucesso.
Ótimo! Agora, complete o checkout para ter acesso completo.
Bem vindo de volta! Você fez login com sucesso.
Parábens! Sua conta está completamente ativada, agora você tem acesso completo ao conteúdo.