SEC Consult SA-20201001-0 :: Broken Access Control in Platinum Mobile

From: SEC Consult Vulnerability Lab <research () sec-consult com>
Date: Fri, 2 Oct 2020 18:17:48 +0000

```
SEC Consult Vulnerability Lab Security Advisory < 20201001-0 >
=======================================================================
             title: Broken Access Control
           product: Platinum Mobile
 vulnerable version: 1.0.4.850
      fixed version: 1.0.4.851
         CVE number: -
             impact: critical
           homepage: https://www.platinumchina.com/en/products/pl1
              found: 2020-04-24
                 by: M. Li (Office Munich)
                     SEC Consult Vulnerability Lab

                     An integrated part of SEC Consult
                     Europe | Asia | North America

                     https://www.sec-consult.com

=======================================================================

Vendor description:
-------------------
"Platinum Mobile is a mobile office system based on Platinum HRM and ESS
Workflow to realize HR informatization management, taking portable devices
such as mobile phone, tablet pc as its main form and carrier. The new mobile
solution will enable employees quickly and conveniently deal with affairs and
not limited by time and place, thus effectively expedite the efficiency of
internal communication and operations. Users can directly use their mobile
devices landing on the client side to complete a series of tasks. Meanwhile,
the executive have the access to making decisions and approvals anytime and
anywhere."

Source: https://www.platinumchina.com/en/products/pl1


Business recommendation:
------------------------
It is recommended to apply the hotfix or update the server component to version
1.0.4.851.


Vulnerability overview/description:
-----------------------------------
1) Broken access control
The mobile application connects to the company-specific server, which does
not properly restrict the access to confidential data. Thus, an authenticated
attacker can disclose the company's payroll, personal information of other
employees without having appropriate privileges to do so.


Proof of concept:
-----------------
1) Broken access control
The mobile application's request consists primarily of two parts: an XML message
in the body and its MD5 hash in the query string.

POST /MobileHandler.ashx?MessageHash=43a98be456b0213ce45e23fdf54c58b8 HTTP/1.1
Host: [redacted]
Content-Length: 276

<Message ID="msg1" MessageType="InvokeServiceMessage" Service="Payslip" Method="getMyPayslipMonthInfoForReleaseMany"
Language="English" UserCode="user0" TokenID=""><Parameters><String>0000000537</String><DateTime>2020-03-31
00:00:00</DateTime><null/></Parameters></Message>

Analyzing the mobile application reveals the following algorithm to
calculate the hash:

MessageHash = hex_md5(escape(XmlMsg) + TokenID);

Furthermore, the server-side part of the application runs the following logic
to verify the message:
- extract the "UserCode" value from the message
- look up the "TokenID" associated with the "UserCode"
- calculate and compare the hash
- if valid, trust and use the parameters in the message, which serves as
  the real reference (rather than the "UserCode") to the business data.

Given this information, an authenticated attacker can craft a message with
an arbitrary value set (e.g. 0000000537) for the element "Parameters" and
calculate the hash with the attacker's "UserCode" and "TokenID".

As a consequence, the pay slip of another employee (e.g. a higher-ranked
manager) can be disclosed. By iterating the values, the attacker can
reveal the entire payroll data of the whole company.

In the following example an authenticated user "user0" can collect
personal information of "user1", including phone number, emails etc.

POST /platinummobile/Handlers/MobileHandler.ashx?MessageHash=bf62c16cad7a6b27b0fee8e1a21409b7 HTTP/1.1
Host: [redacted]
Content-Length: 203

<Message ID="msg1" MessageType="InvokeServiceMessage" Service="MyAccount" Method="GetMyInfo" Language="English"
UserCode="user0" TokenID=""><Parameters><String>user1</String></Parameters></Message>


Vulnerable / tested versions:
-----------------------------
The following version has been tested, which was the most recent one at the
time of the test:
- 1.0.4.864 on Android
- 1.0.4.864 on iOS
- 1.0.4.850 on Server


Vendor contact timeline:
------------------------
2020-05-19: Contact vendor through the provided email address.
2020-05-20: Exchange on the issue.
2020-05-22: Vendor acknowledged the issue, and claimed a hotfix will be released
            before a fix in the next version.
2020-07-22: Contact the vendor again.
2020-07-23: Vendor informed that a hotfix has been released.
```

2020-08-19: Customer confirmed that the hotfix works.
2020-10-01: Release of the advisory.

Solution:

Apply the hotfix or update the application to the latest version 1.0.4.851.

Workaround:

None

Advisory URL:
----
https://www.sec-consult.com/en/Vulnerability-Lab/Advisories.htm

~~~~~~

SEC Consult Vulnerability Lab

SEC Consult
Europe | Asia | North America

About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult. It
ensures the continued knowledge gain of SEC Consult in the field of network
and application security to stay ahead of the attacker. The SEC Consult
Vulnerability Lab supports high-quality penetration testing and the evaluation
of new offensive and defensive technologies for our customers. Hence our
customers obtain the most current information about vulnerabilities and valid
recommendation about the risk profile of new technologies.

~~~~~~
Interested to work with the experts of SEC Consult?
Send us your application https://www.sec-consult.com/en/Career.htm

Interested in improving your cyber security with the experts of SEC Consult?
Contact our local offices https://www.sec-consult.com/en/About/Contact.htm
~~~~~~

Mail: research at sec-consult dot com
Web: https://www.sec-consult.com
Blog: http://blog.sec-consult.com
Twitter: https://twitter.com/sec_consult

EOF M. Li / @2020

~~~~~~