

Dear Alcatel-Lucent Enterprise Customer:

The purpose of this advisory is to address multiple vulnerabilities in OV3600

Advisory Number: ALE-PSA-2015-005

CVE: CVE-2015-1390, CVE-2015-1391, CVE-2015-2201, CVE-2015-2202

TITLE

OV3600 Multiple Vulnerabilities

SUMMARY

Multiple vulnerabilities exist in OV3600. See below for details.

AFFECTED VERSIONS

OV3600 versions prior to 8.0.7

DETAILS

In order to protect customer networks, Alcatel-Lucent Enterprise is providing no specific details in the initial advisory. In accordance with our vulnerability disclosure policy, Alcatel-Lucent Enterprise will update this advisory in 60 days to provide full details of each vulnerability.

Cross-site Scripting Permits Script Execution Inside Administrative Session (CVE-2015-1390)

A cross-site scripting vulnerability permits an unauthenticated user to inject script code that could be executed by an OV3600 administrator while inside an administrative session. While the vulnerability requires no authentication, it does require administrative access to network elements being managed by OV3600. Simply having HTTP access to the OV3600 console is insufficient.

- Severity: High
- Vulnerability Class: Improper Neutralization of Input During Web Page Generation (CWE-79)
- CVSSv2 Overall Score: 7.5
- CVSSv2 Vector: (AV:N/AC:L/Au:N/C:P/I:P/A:P).
- Fix: Fixed in 8.0.7

Bypass of Cross-Site Request Forgery Prevention Mechanisms (CVE-2015-1391)

OV3600 includes protection mechanisms against cross-site request forgery (CSRF) attacks. It is possible for an attacker to bypass these mechanisms by supplying a crafted URL in an HTTPS request. While a CSRF attack is difficult to carry out, a successful attack would allow the attacker to make arbitrary configuration changes to the OV3600 system, including adding new administrative accounts and changing passwords.

- Severity: Medium
- Vulnerability Class: Improper Neutralization of Input during Web Page Generation (CWE-79)
- CVSSv2 Overall Score: 6.8
- CVSSv2 Vector: (AV:N/AC:H/Au:S/C:P/I:C/A:C)
- Fix: Fixed in 8.0.7

VisualRF Remote Command Execution and File Disclosure (CVE-2015-2201)

This vulnerability permits an authenticated administrative user of any privilege level to execute arbitrary commands on the underlying operating system with the privilege level of the web server component. Using this technique, local files can be exported to an external system or network.

- Severity: Medium
- Vulnerability Class: Improper Control of Generation of Code (CWE-94)
- CVSSv2 Overall Score: 6.0
- CVSSv2 Vector: (AV:N/AC:M/Au:S/C:P/I:P/A:P)
- Fix: Fixed in 8.0.7 and 7.7.14.2

Authenticated Privilege Escalation (CVE-2015-2202)

Incorrect input sanitization in OV3600 allows an authenticated administrative user of any privilege level to execute arbitrary commands on the underlying operating system with the privilege level of 'root'. This permits complete compromise of the OV3600 system.

- Severity: High
- Vulnerability Class: Improper Input Validation (CWE-20)
- CVSSv2 Overall Score: 7.1
- CVSSv2 Vector: (AV:N/AC:H/Au:S/C:C/I:C/A:C)
- Fix: Fixed in 8.0.7 and 7.7.14.2

WORKAROUND

There are no completely effective workarounds for these issues.

SOLUTION

Please contact Alcatel-Lucent Enterprise Service & Support for details.

For more detailed information, please go to the following link: <https://service.esd.alcatel-lucent.com>

If you are experiencing problems with your support site login, please send an email detailing this problem to: esd.support@alcatel-lucent.com

Our Commitment to Enhancing Security

The Alcatel-Lucent Enterprise OmniAccess WLAN Switch is distributed in cooperation with Aruba Networks. Alcatel-Lucent Enterprise will continue to work closely with Aruba Networks in order to continuously enhance the security capabilities of the OAW products. Alcatel-Lucent Enterprise will continue to work with its partner to address these issues and communicate the latest updates. If you have any further questions please contact us at:

- Email: esd.support@alcatel-lucent.com
- North America Service and Support: 1-800-995-2696
- Latin America Service and Support: 1-877-919-9526
- European Service and Support: +800 00200100 (Toll Free) or +1(650)385-2193
- Asia Pacific Service and Support: +65-6240-8484
- Other International: 1-878-878-4507