

Stack based buffer overflow in OmniSwitch

Summary

A stack based buffer overflow was discovered within Alcatel-Lucent OmniSwitch products. This buffer overflow was discovered within the embedded management web server and can be exploited remotely without user authentication

Risk analysis

CVSS Score: 0.8

CVSS Base Score	4.3	CVSS Temporal Score	3.2	CVSS Environmental Score	0.8
------------------------	------------	----------------------------	------------	---------------------------------	------------

Affected Products and Configurations

The vulnerability affects the entire Alcatel-Lucent OmniSwitch product line. Specifically, it impacts the following Alcatel OmniSwitch products:

- OS7000 Series
- OS6600 Series
- OS6800 Series
- OS6850 Series
- OS9000 Series

Non-Affected Products and Configurations

Detailed vulnerability description

The vulnerability is triggered by passing the overflow data within the “**Cookie: Session=**” part of the header for http get request.

This appears to overwrite an address pointer on the stack which gives us full control of the instruction pointer. The amount of bytes needed to trigger the overflow varies between AOS versions.

Impact of the vulnerability

A user having IP connectivity to the switch may send crafted http packets to exploit this vulnerability and gain control of instruction pointer without user authentication

Solutions

The cookie session length is now checked in order to prevent instruction pointer access.

Fixed Software Versions/Patches and how to obtain them

The Problem has been fixed in the following maintenance AoS Releases:



- 5.4.1.429.R01 and above
- 5.1.6.463.R02 and above
- 6.1.3.965.R01 and above
- 6.1.5.595.R01 and above
- 6.3.1.966.R01 and above
- Please contact the Alcatel-Lucent Technical Support or your Business Partner for other releases availability

However, not all maintenance release builds are published. A maintenance release is only published after it has integrated several bug fixes and has been fully tested.

Please contact the Alcatel-Lucent Technical Support or your Business Partner for information on latest maintenance releases.

References

Internal reference number: The vulnerability is tracked with the Alcatel-Lucent Problem Report PR 122812

Cert-IST reference number : Cert-IST/AV-2008.333

History

Date of vulnerability notification : may 22nd, 2008

Date of document publishing on our external PSIRT website : august 6th, 2008

Acknowledgements

Alcatel-Lucent would like to thank Deral Heiland from Layered Defense Research to inform us about this vulnerability, for the good cooperation and for acting according to our disclosure policy practices. We encourage others to report any potential vulnerabilities by sending a Vulnerability Summary Report to psirt.security@alcatel-lucent.com. As such we will be able to improve the security characteristics of our products and the environments in which they are deployed.

Vendor Statement

ALU is committed to continuously enhancing our security posture, and we have both internal and external resources involved in security review processes aimed at identifying product vulnerabilities, both in existing and in developing products.

It is important to note that there have been no reports of compromise due to this vulnerability. ALUs primary concern in this instance is to rapidly deploy a solution for our entire customer base. As a result, ALU has released patches for most code versions.

We highly recommend that you upgrade your products to a patch corresponding to your currently installed release. While we encourage customers to always utilize the latest releases to ensure the full benefit of our continued innovation and improvements, we recognize that this is not always possible.

Information on our disclosure policy, how to report vulnerabilities and a list of public advisories can be found at our PSIRT website : <http://www1.alcatel-lucent.com/psirt>