Oce Colorwave 500 CSRF / XSS / Authentication Bypass

Authored by Marco Ortisi, redtimmysec, Giuseppe Cali

Posted Mar 19, 2020

Oce Colorwave 500 printer suffers from authentication bypass, cross site request forgery, and cross site scripting vulnerabilities.

tags | advisory, vulnerability, xss, bypass, csrf
advisories | CVE-2020-10667, CVE-2020-10668, CVE-2020-10669, CVE-2020-10670, CVE-2020-10671
SHA-256 | cb5874cc976834228bc185741becb79371ed3b619e098dbdd4244f3a27610bf7 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Océ Colorwave 500 printer: Multiple vulnerabilities
# Exploit Author: Giuseppe Cali, Marco Ortisi
# Authors blog: https://www.redtimmy.com
# Vendor Homepage: https://www.canon.com
# Software Link:
https://lfpp.csa.canon.com/tss/tss_product_detail.jsp?
PRODUCT%3C%3Eprd_id=845524441910378&SKU%3C%3Esku_id=1689949372031068&FOLDER%3C%3Efolder_id=2534374302162637&bmU
# Version: 4.0.0.0
# CVE: 2020-10667, 2020-10668, 2020-10669, 2020-10670, 2020-10671

We have recently registered five CVE(s) affecting the Oce Colorwave 500
printer.

CVE-2020-10669 is an authentication bypass allowing an attacker to
access
documents that have been uploaded to the printer. As the documents
remain stored
in the system even after they have been printed (depending on the
printer's
configuration), a malicious insider may be able to access documents
printed in
the past.

CVE-2020-10667 is a Stored XSS on the
"/TemplateManager/indexExternalLocation.jsp"
page.

CVE-2020-10668 and CVE-10670 are two Reflected XSS on pages "/home.jsp"
and
"/SettingsEditor/settingDialogContent.jsp".

Finally CVE-10671 is a system-wide CSRF due to the absence of any form
of nonce
or countermeasure protecting against Cross Site Request Forgery.

More details and full story here:
https://www.redtimmy.com/red-teaming/hacking-the-oce-colorwave-printer-when-a-quick-security-assessment-
determines-the-success-of-a-red-team-exercise/
```

Login or Register to add favorites

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 154 files
Ubuntu 73 files
LiquidWorm 23 files
Debian 18 files
malvuln 11 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter

Subscribe to an RSS Feed