

# Xerox Security Bulletin XR17-031



Xerox® FreeFlow® Print Server v9 / Solaris 11

## Supports:

- Xerox® Color 800i/1000i Digital Press
- Xerox® Versant® 3100 Press

Delivery of: October 2017 Security Patch Cluster

Includes: Java 7 Update 161

Bulletin Date: December 20, 2017

## 1.0 Background

Oracle® delivers quarterly Critical Patch Updates (CPU) to address US-CERT-announced Security vulnerabilities and deliver reliability improvements to the Solaris Operating platform. Oracle® does not provide these patches to the public, but authorize vendors like Xerox® to deliver them to Customers with active FreeFlow® Print Server Support Contracts (FSMA). Customers who may have an Oracle® Support Contract for their non-FreeFlow® Print Server Solaris Servers should not install patches not prepared/delivered by Xerox®. Installing non-authorized patches for the FreeFlow® Print Server software violates Oracle® agreements, can render the platform inoperable, and result in downtime and/or a lengthy re-installation service call.

This bulletin announces the availability of the following:

1. **Solaris 11.3 Operating System (OS) Upgrade**
  - This supersedes the Solaris 11.2 OS
  - Required for Color 800i/1000i Presses only.
  - Solaris 11.3 OS already installed for the Xerox® Versant® 3100.
2. **October 2017 Security Patch Cluster**
  - This is the first Security Patch Cluster delivered for the Solaris 11.3 OS.
3. **Java 7 Update 161 Software**
  - This supersedes Java 7 Update 121 Software (Color 800i/1000i Digital Press)
  - Supersedes Java 6 Update 105 Software (Versant® 3100 Press)

**Note:** Solaris 11.2 is the base OS installed for the Xerox® Color 800i/1000i Presses and requires upgrade to the Solaris 11.3 OS before installing the October 2017 Security Patch Cluster. This upgrade is not required for the Xerox® Versant® 3100 given the base OS is already Solaris 11.3.

See US-CERT Common Vulnerability Exposures (CVE) patches installed with Solaris 11.3 OS Upgrade that are remediated in the table below:

| Solaris 11.3 Included Security Patch Remediated US-CERT CVE's |               |               |               |               |                |
|---|---------------|---------------|---------------|---------------|----------------|
| CVE-2013-6370   | CVE-2015-1819 | CVE-2015-2729 | CVE-2015-2737 | CVE-2015-2922 | CVE-2016-0414  |
| CVE-2013-6371   | CVE-2015-2721 | CVE-2015-2730 | CVE-2015-2738 | CVE-2015-2923 | CVE-2016-0416  |
| CVE-2014-2653   | CVE-2015-2722 | CVE-2015-2731 | CVE-2015-2739 | CVE-2015-3900 | CVE-2016-0418  |
| CVE-2014-3564   | CVE-2015-2724 | CVE-2015-2733 | CVE-2015-2740 | CVE-2015-4020 | CVE-2016-0419  |
| CVE-2014-3566   | CVE-2015-2725 | CVE-2015-2734 | CVE-2015-2741 | CVE-2015-4920 | CVE-2016-0426  |
| CVE-2014-3634   | CVE-2015-2726 | CVE-2015-2735 | CVE-2015-2742 | CVE-2015-5600 | CVE-2016-0431  |
| CVE-2014-3683   | CVE-2015-2728 | CVE-2015-2736 | CVE-2015-2743 | CVE-2016-0403 | CVE-2017-10003 |

See US-CERT Common Vulnerability Exposures (CVE) the October 2017 Security Patch Cluster remediate in table below:

| October 2017 Security Patch Cluster Remediated US-CERT CVE's |               |               |               |               |               |
|--|---------------|---------------|---------------|---------------|---------------|
| CVE-2013-1438  | CVE-2015-1547 | CVE-2015-7853 | CVE-2016-2838 | CVE-2016-7536 | CVE-2017-3652 |
| CVE-2013-1511  | CVE-2015-1782 | CVE-2015-7854 | CVE-2016-2839 | CVE-2016-7537 | CVE-2017-3653 |
| CVE-2013-5609  | CVE-2015-2566 | CVE-2015-7855 | CVE-2016-2842 | CVE-2016-7538 | CVE-2017-3731 |
| CVE-2013-5610  | CVE-2015-2567 | CVE-2015-7871 | CVE-2016-3115 | CVE-2016-7539 | CVE-2017-3732 |
| CVE-2013-5611  | CVE-2015-2568 | CVE-2015-7942 | CVE-2016-3120 | CVE-2016-7540 | CVE-2017-5202 |
| CVE-2013-5612  | CVE-2015-2571 | CVE-2015-7973 | CVE-2016-3189 | CVE-2016-7543 | CVE-2017-5203 |
| CVE-2013-5613  | CVE-2015-2573 | CVE-2015-7974 | CVE-2016-3191 | CVE-2016-7799 | CVE-2017-5204 |
| CVE-2013-5614  | CVE-2015-2582 | CVE-2015-7975 | CVE-2016-3424 | CVE-2016-7906 | CVE-2017-5205 |
| CVE-2013-5615  | CVE-2015-2611 | CVE-2015-7976 | CVE-2016-3440 | CVE-2016-7922 | CVE-2017-5341 |
| CVE-2013-5616  | CVE-2015-2617 | CVE-2015-7977 | CVE-2016-3452 | CVE-2016-7923 | CVE-2017-5342 |
| CVE-2013-5618  | CVE-2015-2620 | CVE-2015-7978 | CVE-2016-3459 | CVE-2016-7924 | CVE-2017-5373 |
| CVE-2013-5619  | CVE-2015-2639 | CVE-2015-7979 | CVE-2016-3465 | CVE-2016-7925 | CVE-2017-5375 |
| CVE-2013-6629  | CVE-2015-2641 | CVE-2015-7981 | CVE-2016-3486 | CVE-2016-7926 | CVE-2017-5376 |
| CVE-2013-6630  | CVE-2015-2643 | CVE-2015-7995 | CVE-2016-3492 | CVE-2016-7927 | CVE-2017-5378 |
| CVE-2013-6671  | CVE-2015-2648 | CVE-2015-8025 | CVE-2016-3495 | CVE-2016-7928 | CVE-2017-5380 |
| CVE-2013-6672  | CVE-2015-2661 | CVE-2015-8107 | CVE-2016-3497 | CVE-2016-7929 | CVE-2017-5383 |
| CVE-2013-6673  | CVE-2015-2706 | CVE-2015-8126 | CVE-2016-3501 | CVE-2016-7930 | CVE-2017-5386 |
| CVE-2013-7447  | CVE-2015-2708 | CVE-2015-8138 | CVE-2016-3518 | CVE-2016-7931 | CVE-2017-5390 |
| CVE-2014-1477  | CVE-2015-2709 | CVE-2015-8139 | CVE-2016-3588 | CVE-2016-7932 | CVE-2017-5396 |
| CVE-2014-1478  | CVE-2015-2710 | CVE-2015-8140 | CVE-2016-3614 | CVE-2016-7933 | CVE-2017-5398 |
| CVE-2014-1479  | CVE-2015-2711 | CVE-2015-8158 | CVE-2016-3615 | CVE-2016-7934 | CVE-2017-5399 |
| CVE-2014-1480  | CVE-2015-2712 | CVE-2015-8241 | CVE-2016-3627 | CVE-2016-7935 | CVE-2017-5400 |
| CVE-2014-1481  | CVE-2015-2713 | CVE-2015-8242 | CVE-2016-3705 | CVE-2016-7936 | CVE-2017-5401 |
| CVE-2014-1482  | CVE-2015-2714 | CVE-2015-8317 | CVE-2016-3714 | CVE-2016-7937 | CVE-2017-5402 |
| CVE-2014-1483  | CVE-2015-2715 | CVE-2015-8540 | CVE-2016-3715 | CVE-2016-7938 | CVE-2017-5403 |
| CVE-2014-1484  | CVE-2015-2716 | CVE-2015-8605 | CVE-2016-3716 | CVE-2016-7939 | CVE-2017-5404 |
| CVE-2014-1485  | CVE-2015-2717 | CVE-2015-8607 | CVE-2016-3717 | CVE-2016-7940 | CVE-2017-5405 |
| CVE-2014-1486  | CVE-2015-2718 | CVE-2015-8665 | CVE-2016-3718 | CVE-2016-7942 | CVE-2017-5406 |
| CVE-2014-1487  | CVE-2015-2720 | CVE-2015-8683 | CVE-2016-4006 | CVE-2016-7943 | CVE-2017-5407 |
| CVE-2014-1488  | CVE-2015-2721 | CVE-2015-8704 | CVE-2016-4078 | CVE-2016-7944 | CVE-2017-5408 |
| CVE-2014-1489  | CVE-2015-2722 | CVE-2015-8705 | CVE-2016-4079 | CVE-2016-7945 | CVE-2017-5409 |
| CVE-2014-1493  | CVE-2015-2724 | CVE-2015-8711 | CVE-2016-4080 | CVE-2016-7946 | CVE-2017-5410 |
| CVE-2014-1494  | CVE-2015-2725 | CVE-2015-8712 | CVE-2016-4081 | CVE-2016-7947 | CVE-2017-5411 |
| CVE-2014-1496  | CVE-2015-2726 | CVE-2015-8713 | CVE-2016-4082 | CVE-2016-7948 | CVE-2017-5412 |
| CVE-2014-1497  | CVE-2015-2727 | CVE-2015-8714 | CVE-2016-4300 | CVE-2016-7949 | CVE-2017-5413 |
| CVE-2014-1498  | CVE-2015-2728 | CVE-2015-8715 | CVE-2016-4301 | CVE-2016-7950 | CVE-2017-5414 |
| CVE-2014-1499  | CVE-2015-2729 | CVE-2015-8716 | CVE-2016-4302 | CVE-2016-7951 | CVE-2017-5416 |
| CVE-2014-1500  | CVE-2015-2730 | CVE-2015-8717 | CVE-2016-4417 | CVE-2016-7952 | CVE-2017-5418 |

|               |               |               |               |               |               |
|---------------|---------------|---------------|---------------|---------------|---------------|
| CVE-2014-1501 | CVE-2015-2731 | CVE-2015-8718 | CVE-2016-4418 | CVE-2016-7953 | CVE-2017-5419 |
| CVE-2014-1502 | CVE-2015-2733 | CVE-2015-8719 | CVE-2016-4421 | CVE-2016-7973 | CVE-2017-5421 |
| CVE-2014-1504 | CVE-2015-2734 | CVE-2015-8720 | CVE-2016-4447 | CVE-2016-7974 | CVE-2017-5422 |
| CVE-2014-1505 | CVE-2015-2735 | CVE-2015-8721 | CVE-2016-4448 | CVE-2016-7975 | CVE-2017-5425 |
| CVE-2014-1506 | CVE-2015-2736 | CVE-2015-8722 | CVE-2016-4449 | CVE-2016-7983 | CVE-2017-5426 |
| CVE-2014-1507 | CVE-2015-2737 | CVE-2015-8723 | CVE-2016-4456 | CVE-2016-7984 | CVE-2017-5429 |
| CVE-2014-1508 | CVE-2015-2738 | CVE-2015-8724 | CVE-2016-4483 | CVE-2016-7985 | CVE-2017-5432 |
| CVE-2014-1509 | CVE-2015-2739 | CVE-2015-8725 | CVE-2016-4562 | CVE-2016-7986 | CVE-2017-5433 |
| CVE-2014-1510 | CVE-2015-2740 | CVE-2015-8726 | CVE-2016-4563 | CVE-2016-7992 | CVE-2017-5434 |
| CVE-2014-1511 | CVE-2015-2741 | CVE-2015-8727 | CVE-2016-4564 | CVE-2016-7993 | CVE-2017-5435 |
| CVE-2014-1512 | CVE-2015-2742 | CVE-2015-8728 | CVE-2016-4953 | CVE-2016-8283 | CVE-2017-5436 |
| CVE-2014-1513 | CVE-2015-2743 | CVE-2015-8729 | CVE-2016-4954 | CVE-2016-8284 | CVE-2017-5437 |
| CVE-2014-1514 | CVE-2015-2806 | CVE-2015-8730 | CVE-2016-4955 | CVE-2016-8286 | CVE-2017-5438 |
| CVE-2014-1518 | CVE-2015-3183 | CVE-2015-8731 | CVE-2016-4956 | CVE-2016-8287 | CVE-2017-5439 |
| CVE-2014-1519 | CVE-2015-3185 | CVE-2015-8732 | CVE-2016-4957 | CVE-2016-8288 | CVE-2017-5440 |
| CVE-2014-1520 | CVE-2015-3194 | CVE-2015-8733 | CVE-2016-4971 | CVE-2016-8289 | CVE-2017-5441 |
| CVE-2014-1522 | CVE-2015-3195 | CVE-2015-8781 | CVE-2016-4979 | CVE-2016-8290 | CVE-2017-5442 |
| CVE-2014-1523 | CVE-2015-3196 | CVE-2015-8782 | CVE-2016-5010 | CVE-2016-8318 | CVE-2017-5443 |
| CVE-2014-1524 | CVE-2015-3210 | CVE-2015-8783 | CVE-2016-5118 | CVE-2016-8327 | CVE-2017-5444 |
| CVE-2014-1525 | CVE-2015-3217 | CVE-2015-8784 | CVE-2016-5239 | CVE-2016-8330 | CVE-2017-5445 |
| CVE-2014-1526 | CVE-2015-3228 | CVE-2015-8806 | CVE-2016-5250 | CVE-2016-8574 | CVE-2017-5446 |
| CVE-2014-1527 | CVE-2015-3885 | CVE-2015-8853 | CVE-2016-5252 | CVE-2016-8575 | CVE-2017-5447 |
| CVE-2014-1528 | CVE-2015-4000 | CVE-2015-8895 | CVE-2016-5254 | CVE-2016-8610 | CVE-2017-5448 |
| CVE-2014-1529 | CVE-2015-4473 | CVE-2015-8896 | CVE-2016-5257 | CVE-2016-8707 | CVE-2017-5459 |
| CVE-2014-1530 | CVE-2015-4474 | CVE-2015-8897 | CVE-2016-5258 | CVE-2016-8740 | CVE-2017-5460 |
| CVE-2014-1531 | CVE-2015-4475 | CVE-2015-8898 | CVE-2016-5259 | CVE-2016-8743 | CVE-2017-5461 |
| CVE-2014-1532 | CVE-2015-4476 | CVE-2015-8934 | CVE-2016-5261 | CVE-2016-8826 | CVE-2017-5462 |
| CVE-2014-1533 | CVE-2015-4477 | CVE-2015-8948 | CVE-2016-5262 | CVE-2016-8862 | CVE-2017-5464 |
| CVE-2014-1534 | CVE-2015-4478 | CVE-2015-8957 | CVE-2016-5263 | CVE-2016-8864 | CVE-2017-5465 |
| CVE-2014-1536 | CVE-2015-4479 | CVE-2015-8958 | CVE-2016-5264 | CVE-2016-9042 | CVE-2017-5469 |
| CVE-2014-1537 | CVE-2015-4480 | CVE-2015-8959 | CVE-2016-5265 | CVE-2016-9064 | CVE-2017-5470 |
| CVE-2014-1538 | CVE-2015-4481 | CVE-2016-0440 | CVE-2016-5270 | CVE-2016-9066 | CVE-2017-5472 |
| CVE-2014-1539 | CVE-2015-4482 | CVE-2016-0505 | CVE-2016-5272 | CVE-2016-9074 | CVE-2017-5482 |
| CVE-2014-1540 | CVE-2015-4483 | CVE-2016-0546 | CVE-2016-5274 | CVE-2016-9079 | CVE-2017-5483 |
| CVE-2014-1541 | CVE-2015-4484 | CVE-2016-0596 | CVE-2016-5276 | CVE-2016-9131 | CVE-2017-5484 |
| CVE-2014-1542 | CVE-2015-4485 | CVE-2016-0597 | CVE-2016-5277 | CVE-2016-9147 | CVE-2017-5485 |
| CVE-2014-1543 | CVE-2015-4486 | CVE-2016-0598 | CVE-2016-5278 | CVE-2016-9243 | CVE-2017-5486 |
| CVE-2014-1544 | CVE-2015-4487 | CVE-2016-0600 | CVE-2016-5280 | CVE-2016-9298 | CVE-2017-5506 |
| CVE-2014-1545 | CVE-2015-4488 | CVE-2016-0606 | CVE-2016-5281 | CVE-2016-9310 | CVE-2017-5507 |
| CVE-2014-1547 | CVE-2015-4489 | CVE-2016-0608 | CVE-2016-5284 | CVE-2016-9311 | CVE-2017-5508 |
| CVE-2014-1548 | CVE-2015-4490 | CVE-2016-0609 | CVE-2016-5290 | CVE-2016-9312 | CVE-2017-5509 |

|               |               |                  |               |               |               |
|---------------|---------------|------------------|---------------|---------------|---------------|
| CVE-2014-1549 | CVE-2015-4491 | CVE-2016-0616    | CVE-2016-5291 | CVE-2016-9372 | CVE-2017-5510 |
| CVE-2014-1550 | CVE-2015-4492 | CVE-2016-0634    | CVE-2016-5294 | CVE-2016-9373 | CVE-2017-5511 |
| CVE-2014-1551 | CVE-2015-4493 | CVE-2016-0702    | CVE-2016-5296 | CVE-2016-9374 | CVE-2017-5596 |
| CVE-2014-1552 | CVE-2015-4495 | CVE-2016-0705    | CVE-2016-5297 | CVE-2016-9375 | CVE-2017-5597 |
| CVE-2014-1553 | CVE-2015-4496 | CVE-2016-0736    | CVE-2016-5350 | CVE-2016-9376 | CVE-2017-5618 |
| CVE-2014-1554 | CVE-2015-4497 | CVE-2016-0787    | CVE-2016-5351 | CVE-2016-9401 | CVE-2017-6014 |
| CVE-2014-1555 | CVE-2015-4498 | CVE-2016-0797    | CVE-2016-5352 | CVE-2016-9422 | CVE-2017-6451 |
| CVE-2014-1556 | CVE-2015-4500 | CVE-2016-0798    | CVE-2016-5353 | CVE-2016-9423 | CVE-2017-6452 |
| CVE-2014-1557 | CVE-2015-4501 | CVE-2016-0799    | CVE-2016-5354 | CVE-2016-9424 | CVE-2017-6455 |
| CVE-2014-1559 | CVE-2015-4502 | CVE-2016-1000104 | CVE-2016-5355 | CVE-2016-9425 | CVE-2017-6458 |
| CVE-2014-1561 | CVE-2015-4503 | CVE-2016-10087   | CVE-2016-5356 | CVE-2016-9426 | CVE-2017-6459 |
| CVE-2014-1562 | CVE-2015-4504 | CVE-2016-10144   | CVE-2016-5357 | CVE-2016-9428 | CVE-2017-6460 |
| CVE-2014-1563 | CVE-2015-4505 | CVE-2016-10145   | CVE-2016-5358 | CVE-2016-9429 | CVE-2017-6462 |
| CVE-2014-1564 | CVE-2015-4506 | CVE-2016-10146   | CVE-2016-5384 | CVE-2016-9430 | CVE-2017-6463 |
| CVE-2014-1565 | CVE-2015-4507 | CVE-2016-10164   | CVE-2016-5387 | CVE-2016-9431 | CVE-2017-6464 |
| CVE-2014-1566 | CVE-2015-4508 | CVE-2016-10252   | CVE-2016-5407 | CVE-2016-9432 | CVE-2017-6467 |
| CVE-2014-1567 | CVE-2015-4509 | CVE-2016-10328   | CVE-2016-5436 | CVE-2016-9433 | CVE-2017-6468 |
| CVE-2014-1568 | CVE-2015-4510 | CVE-2016-10349   | CVE-2016-5437 | CVE-2016-9434 | CVE-2017-6469 |
| CVE-2014-1569 | CVE-2015-4511 | CVE-2016-10350   | CVE-2016-5439 | CVE-2016-9435 | CVE-2017-6470 |
| CVE-2014-1575 | CVE-2015-4512 | CVE-2016-1238    | CVE-2016-5440 | CVE-2016-9436 | CVE-2017-6471 |
| CVE-2014-1580 | CVE-2015-4513 | CVE-2016-1248    | CVE-2016-5441 | CVE-2016-9437 | CVE-2017-6472 |
| CVE-2014-1582 | CVE-2015-4514 | CVE-2016-1283    | CVE-2016-5442 | CVE-2016-9438 | CVE-2017-6473 |
| CVE-2014-1584 | CVE-2015-4515 | CVE-2016-1285    | CVE-2016-5443 | CVE-2016-9439 | CVE-2017-6474 |
| CVE-2014-1588 | CVE-2015-4516 | CVE-2016-1286    | CVE-2016-5444 | CVE-2016-9440 | CVE-2017-7186 |
| CVE-2014-1589 | CVE-2015-4517 | CVE-2016-1523    | CVE-2016-5469 | CVE-2016-9441 | CVE-2017-7244 |
| CVE-2014-1591 | CVE-2015-4518 | CVE-2016-1541    | CVE-2016-5471 | CVE-2016-9442 | CVE-2017-7245 |
| CVE-2014-1595 | CVE-2015-4519 | CVE-2016-1546    | CVE-2016-5507 | CVE-2016-9443 | CVE-2017-7246 |
| CVE-2014-2018 | CVE-2015-4520 | CVE-2016-1547    | CVE-2016-5559 | CVE-2016-9444 | CVE-2017-7507 |
| CVE-2014-2432 | CVE-2015-4521 | CVE-2016-1548    | CVE-2016-5561 | CVE-2016-9556 | CVE-2017-7526 |
| CVE-2014-2440 | CVE-2015-4522 | CVE-2016-1549    | CVE-2016-5584 | CVE-2016-9559 | CVE-2017-7586 |
| CVE-2014-2494 | CVE-2015-4651 | CVE-2016-1550    | CVE-2016-5598 | CVE-2016-9584 | CVE-2017-7619 |
| CVE-2014-3532 | CVE-2015-4652 | CVE-2016-1551    | CVE-2016-5609 | CVE-2016-9621 | CVE-2017-7659 |
| CVE-2014-3533 | CVE-2015-4737 | CVE-2016-1762    | CVE-2016-5612 | CVE-2016-9622 | CVE-2017-7668 |
| CVE-2014-3566 | CVE-2015-4752 | CVE-2016-1833    | CVE-2016-5616 | CVE-2016-9623 | CVE-2017-7679 |
| CVE-2014-3569 | CVE-2015-4756 | CVE-2016-1835    | CVE-2016-5617 | CVE-2016-9624 | CVE-2017-7700 |
| CVE-2014-3635 | CVE-2015-4761 | CVE-2016-1836    | CVE-2016-5624 | CVE-2016-9625 | CVE-2017-7701 |
| CVE-2014-3636 | CVE-2015-4767 | CVE-2016-1837    | CVE-2016-5625 | CVE-2016-9626 | CVE-2017-7702 |
| CVE-2014-3637 | CVE-2015-4769 | CVE-2016-1838    | CVE-2016-5626 | CVE-2016-9627 | CVE-2017-7703 |
| CVE-2014-3638 | CVE-2015-4771 | CVE-2016-1839    | CVE-2016-5627 | CVE-2016-9628 | CVE-2017-7704 |
| CVE-2014-3639 | CVE-2015-4772 | CVE-2016-1840    | CVE-2016-5628 | CVE-2016-9629 | CVE-2017-7705 |
| CVE-2014-4243 | CVE-2015-4792 | CVE-2016-1930    | CVE-2016-5629 | CVE-2016-9630 | CVE-2017-7742 |

|               |               |               |               |                |               |
|---------------|---------------|---------------|---------------|----------------|---------------|
| CVE-2014-4260 | CVE-2015-4802 | CVE-2016-1931 | CVE-2016-5630 | CVE-2016-9631  | CVE-2017-7745 |
| CVE-2014-4287 | CVE-2015-4807 | CVE-2016-1935 | CVE-2016-5631 | CVE-2016-9632  | CVE-2017-7746 |
| CVE-2014-6464 | CVE-2015-4815 | CVE-2016-1938 | CVE-2016-5632 | CVE-2016-9633  | CVE-2017-7747 |
| CVE-2014-6469 | CVE-2015-4816 | CVE-2016-1950 | CVE-2016-5633 | CVE-2016-9840  | CVE-2017-7748 |
| CVE-2014-6484 | CVE-2015-4819 | CVE-2016-1952 | CVE-2016-5634 | CVE-2016-9841  | CVE-2017-7749 |
| CVE-2014-6491 | CVE-2015-4826 | CVE-2016-1953 | CVE-2016-5635 | CVE-2016-9842  | CVE-2017-7750 |
| CVE-2014-6494 | CVE-2015-4830 | CVE-2016-1954 | CVE-2016-5687 | CVE-2016-9843  | CVE-2017-7751 |
| CVE-2014-6496 | CVE-2015-4836 | CVE-2016-1955 | CVE-2016-5688 | CVE-2016-9844  | CVE-2017-7752 |
| CVE-2014-6500 | CVE-2015-4858 | CVE-2016-1956 | CVE-2016-5689 | CVE-2016-9893  | CVE-2017-7753 |
| CVE-2014-6505 | CVE-2015-4861 | CVE-2016-1957 | CVE-2016-5690 | CVE-2016-9895  | CVE-2017-7754 |
| CVE-2014-6507 | CVE-2015-4864 | CVE-2016-1958 | CVE-2016-5691 | CVE-2016-9897  | CVE-2017-7755 |
| CVE-2014-6520 | CVE-2015-4870 | CVE-2016-1960 | CVE-2016-5824 | CVE-2016-9898  | CVE-2017-7756 |
| CVE-2014-6530 | CVE-2015-4879 | CVE-2016-1961 | CVE-2016-5841 | CVE-2016-9899  | CVE-2017-7757 |
| CVE-2014-6555 | CVE-2015-4913 | CVE-2016-1962 | CVE-2016-5842 | CVE-2016-9900  | CVE-2017-7758 |
| CVE-2014-6559 | CVE-2015-4920 | CVE-2016-1964 | CVE-2016-5844 | CVE-2016-9901  | CVE-2017-7760 |
| CVE-2014-6568 | CVE-2015-5146 | CVE-2016-1965 | CVE-2016-5844 | CVE-2016-9902  | CVE-2017-7761 |
| CVE-2014-7824 | CVE-2015-5300 | CVE-2016-1966 | CVE-2016-6185 | CVE-2016-9904  | CVE-2017-7763 |
| CVE-2014-8631 | CVE-2015-5312 | CVE-2016-1967 | CVE-2016-6261 | CVE-2016-9905  | CVE-2017-7764 |
| CVE-2014-8632 | CVE-2015-5602 | CVE-2016-1969 | CVE-2016-6262 | CVE-2017-0309  | CVE-2017-7765 |
| CVE-2014-8635 | CVE-2015-5621 | CVE-2016-1974 | CVE-2016-6263 | CVE-2017-0310  | CVE-2017-7766 |
| CVE-2014-8636 | CVE-2015-5950 | CVE-2016-1977 | CVE-2016-6302 | CVE-2017-0311  | CVE-2017-7767 |
| CVE-2014-8637 | CVE-2015-6241 | CVE-2016-1978 | CVE-2016-6303 | CVE-2017-0318  | CVE-2017-7768 |
| CVE-2014-8640 | CVE-2015-6242 | CVE-2016-1979 | CVE-2016-6304 | CVE-2017-0321  | CVE-2017-7778 |
| CVE-2014-8642 | CVE-2015-6243 | CVE-2016-2073 | CVE-2016-6305 | CVE-2017-0350  | CVE-2017-7779 |
| CVE-2014-8643 | CVE-2015-6244 | CVE-2016-2105 | CVE-2016-6306 | CVE-2017-0351  | CVE-2017-7782 |
| CVE-2014-9330 | CVE-2015-6245 | CVE-2016-2106 | CVE-2016-6307 | CVE-2017-0352  | CVE-2017-7784 |
| CVE-2014-9512 | CVE-2015-6246 | CVE-2016-2107 | CVE-2016-6308 | CVE-2017-10004 | CVE-2017-7785 |
| CVE-2014-9655 | CVE-2015-6247 | CVE-2016-2108 | CVE-2016-6309 | CVE-2017-10042 | CVE-2017-7786 |
| CVE-2014-9766 | CVE-2015-6248 | CVE-2016-2109 | CVE-2016-6313 | CVE-2017-10095 | CVE-2017-7787 |
| CVE-2014-9848 | CVE-2015-6249 | CVE-2016-2123 | CVE-2016-6491 | CVE-2017-10122 | CVE-2017-7791 |
| CVE-2014-9849 | CVE-2015-7174 | CVE-2016-2125 | CVE-2016-6503 | CVE-2017-11108 | CVE-2017-7792 |
| CVE-2014-9852 | CVE-2015-7175 | CVE-2016-2126 | CVE-2016-6504 | CVE-2017-11406 | CVE-2017-7793 |
| CVE-2014-9853 | CVE-2015-7176 | CVE-2016-2161 | CVE-2016-6505 | CVE-2017-11407 | CVE-2017-7798 |
| CVE-2014-9854 | CVE-2015-7177 | CVE-2016-2176 | CVE-2016-6506 | CVE-2017-11408 | CVE-2017-7800 |
| CVE-2014-9913 | CVE-2015-7178 | CVE-2016-2177 | CVE-2016-6507 | CVE-2017-11410 | CVE-2017-7801 |
| CVE-2015-0228 | CVE-2015-7179 | CVE-2016-2178 | CVE-2016-6508 | CVE-2017-11411 | CVE-2017-7802 |
| CVE-2015-0245 | CVE-2015-7180 | CVE-2016-2179 | CVE-2016-6509 | CVE-2017-12150 | CVE-2017-7803 |
| CVE-2015-0253 | CVE-2015-7181 | CVE-2016-2180 | CVE-2016-6510 | CVE-2017-12151 | CVE-2017-7804 |
| CVE-2015-0374 | CVE-2015-7182 | CVE-2016-2181 | CVE-2016-6511 | CVE-2017-12163 | CVE-2017-7805 |
| CVE-2015-0381 | CVE-2015-7183 | CVE-2016-2182 | CVE-2016-6512 | CVE-2017-1256  | CVE-2017-7807 |
| CVE-2015-0382 | CVE-2015-7184 | CVE-2016-2183 | CVE-2016-6513 | CVE-2017-1376  | CVE-2017-7809 |

|               |               |               |               |                |               |
|---------------|---------------|---------------|---------------|----------------|---------------|
| CVE-2015-0385 | CVE-2015-7185 | CVE-2016-2334 | CVE-2016-6662 | CVE-2017-13766 | CVE-2017-7810 |
| CVE-2015-0391 | CVE-2015-7186 | CVE-2016-2335 | CVE-2016-6823 | CVE-2017-13767 | CVE-2017-7814 |
| CVE-2015-0405 | CVE-2015-7187 | CVE-2016-2381 | CVE-2016-6855 | CVE-2017-3167  | CVE-2017-7818 |
| CVE-2015-0411 | CVE-2015-7188 | CVE-2016-2516 | CVE-2016-7052 | CVE-2017-3169  | CVE-2017-7819 |
| CVE-2015-0423 | CVE-2015-7189 | CVE-2016-2517 | CVE-2016-7055 | CVE-2017-3238  | CVE-2017-7823 |
| CVE-2015-0432 | CVE-2015-7190 | CVE-2016-2518 | CVE-2016-7076 | CVE-2017-3243  | CVE-2017-7824 |
| CVE-2015-0433 | CVE-2015-7191 | CVE-2016-2519 | CVE-2016-7101 | CVE-2017-3244  | CVE-2017-7825 |
| CVE-2015-0438 | CVE-2015-7192 | CVE-2016-2521 | CVE-2016-7175 | CVE-2017-3251  | CVE-2017-8105 |
| CVE-2015-0439 | CVE-2015-7193 | CVE-2016-2530 | CVE-2016-7176 | CVE-2017-3256  | CVE-2017-8287 |
| CVE-2015-0441 | CVE-2015-7194 | CVE-2016-2531 | CVE-2016-7177 | CVE-2017-3257  | CVE-2017-8343 |
| CVE-2015-0498 | CVE-2015-7195 | CVE-2016-2532 | CVE-2016-7178 | CVE-2017-3258  | CVE-2017-8344 |
| CVE-2015-0499 | CVE-2015-7196 | CVE-2016-2766 | CVE-2016-7179 | CVE-2017-3265  | CVE-2017-8345 |
| CVE-2015-0500 | CVE-2015-7197 | CVE-2016-2774 | CVE-2016-7180 | CVE-2017-3273  | CVE-2017-8346 |
| CVE-2015-0503 | CVE-2015-7198 | CVE-2016-2775 | CVE-2016-7382 | CVE-2017-3291  | CVE-2017-8347 |
| CVE-2015-0505 | CVE-2015-7199 | CVE-2016-2776 | CVE-2016-7389 | CVE-2017-3301  | CVE-2017-8348 |
| CVE-2015-0506 | CVE-2015-7200 | CVE-2016-2790 | CVE-2016-7426 | CVE-2017-3302  | CVE-2017-8349 |
| CVE-2015-0507 | CVE-2015-7201 | CVE-2016-2791 | CVE-2016-7427 | CVE-2017-3305  | CVE-2017-8350 |
| CVE-2015-0508 | CVE-2015-7202 | CVE-2016-2792 | CVE-2016-7428 | CVE-2017-3308  | CVE-2017-8351 |
| CVE-2015-0511 | CVE-2015-7205 | CVE-2016-2793 | CVE-2016-7429 | CVE-2017-3309  | CVE-2017-8352 |
| CVE-2015-0797 | CVE-2015-7207 | CVE-2016-2794 | CVE-2016-7431 | CVE-2017-3312  | CVE-2017-8353 |
| CVE-2015-0798 | CVE-2015-7210 | CVE-2016-2795 | CVE-2016-7433 | CVE-2017-3313  | CVE-2017-8354 |
| CVE-2015-0799 | CVE-2015-7212 | CVE-2016-2796 | CVE-2016-7434 | CVE-2017-3317  | CVE-2017-8355 |
| CVE-2015-0800 | CVE-2015-7213 | CVE-2016-2797 | CVE-2016-7440 | CVE-2017-3318  | CVE-2017-8356 |
| CVE-2015-0802 | CVE-2015-7214 | CVE-2016-2798 | CVE-2016-7444 | CVE-2017-3319  | CVE-2017-8357 |
| CVE-2015-0803 | CVE-2015-7222 | CVE-2016-2799 | CVE-2016-7513 | CVE-2017-3320  | CVE-2017-8361 |
| CVE-2015-0804 | CVE-2015-7497 | CVE-2016-2800 | CVE-2016-7514 | CVE-2017-3329  | CVE-2017-8362 |
| CVE-2015-0805 | CVE-2015-7498 | CVE-2016-2801 | CVE-2016-7515 | CVE-2017-3453  | CVE-2017-8363 |
| CVE-2015-0806 | CVE-2015-7499 | CVE-2016-2802 | CVE-2016-7516 | CVE-2017-3456  | CVE-2017-8365 |
| CVE-2015-0808 | CVE-2015-7500 | CVE-2016-2804 | CVE-2016-7517 | CVE-2017-3461  | CVE-2017-8765 |
| CVE-2015-0810 | CVE-2015-7511 | CVE-2016-2805 | CVE-2016-7518 | CVE-2017-3462  | CVE-2017-8830 |
| CVE-2015-0811 | CVE-2015-7575 | CVE-2016-2806 | CVE-2016-7519 | CVE-2017-3463  | CVE-2017-9098 |
| CVE-2015-0812 | CVE-2015-7691 | CVE-2016-2807 | CVE-2016-7520 | CVE-2017-3464  | CVE-2017-9343 |
| CVE-2015-0814 | CVE-2015-7692 | CVE-2016-2808 | CVE-2016-7521 | CVE-2017-3498  | CVE-2017-9344 |
| CVE-2015-0819 | CVE-2015-7696 | CVE-2016-2814 | CVE-2016-7522 | CVE-2017-3510  | CVE-2017-9345 |
| CVE-2015-0820 | CVE-2015-7697 | CVE-2016-2815 | CVE-2016-7523 | CVE-2017-3516  | CVE-2017-9346 |
| CVE-2015-0821 | CVE-2015-7701 | CVE-2016-2818 | CVE-2016-7524 | CVE-2017-3600  | CVE-2017-9347 |
| CVE-2015-0823 | CVE-2015-7702 | CVE-2016-2819 | CVE-2016-7525 | CVE-2017-3629  | CVE-2017-9348 |
| CVE-2015-0824 | CVE-2015-7703 | CVE-2016-2821 | CVE-2016-7526 | CVE-2017-3630  | CVE-2017-9349 |
| CVE-2015-0825 | CVE-2015-7704 | CVE-2016-2822 | CVE-2016-7527 | CVE-2017-3631  | CVE-2017-9350 |
| CVE-2015-0826 | CVE-2015-7705 | CVE-2016-2824 | CVE-2016-7528 | CVE-2017-3634  | CVE-2017-9351 |
| CVE-2015-0828 | CVE-2015-7744 | CVE-2016-2826 | CVE-2016-7529 | CVE-2017-3635  | CVE-2017-9352 |

|               |               |               |               |               |               |
|---------------|---------------|---------------|---------------|---------------|---------------|
| CVE-2015-0829 | CVE-2015-7830 | CVE-2016-2828 | CVE-2016-7530 | CVE-2017-3636 | CVE-2017-9353 |
| CVE-2015-0830 | CVE-2015-7848 | CVE-2016-2830 | CVE-2016-7531 | CVE-2016-7532 | CVE-2017-9354 |
| CVE-2015-0832 | CVE-2015-7849 | CVE-2016-2831 | CVE-2016-2835 | CVE-2016-7533 | CVE-2017-9788 |
| CVE-2015-0833 | CVE-2015-7850 | CVE-2015-7851 | CVE-2016-2836 | CVE-2017-3641 | CVE-2017-9789 |
| CVE-2015-0834 | CVE-2015-0835 | CVE-2015-7852 | CVE-2016-7532 | CVE-2017-3647 | CVE-2017-3652 |
| CVE-2013-1438 | CVE-2015-1547 | CVE-2016-2835 | CVE-2016-7533 | CVE-2017-3648 | CVE-2017-3653 |
| CVE-2013-1511 | CVE-2015-7851 | CVE-2016-2836 | CVE-2016-7534 | CVE-2017-3649 | CVE-2017-3731 |
| CVE-2015-0835 | CVE-2015-7852 | CVE-2016-2837 | CVE-2016-7535 | CVE-2017-3651 |               |

See the US-CERT Common Vulnerability Exposures (CVE) the Java 7 Update 161 Software remediate in table below:

| Java 7 Update 161 Software Remediated US-CERT CVE's |               |               |               |               |               |
|---|---------------|---------------|---------------|---------------|---------------|
| CVE-2013-1500                                       | CVE-2013-2443 | CVE-2013-2450 | CVE-2013-2456 | CVE-2013-2464 | CVE-2013-2470 |
| CVE-2013-1571                                       | CVE-2013-2444 | CVE-2013-2451 | CVE-2013-2457 | CVE-2013-2465 | CVE-2013-2471 |
| CVE-2013-2407                                       | CVE-2013-2445 | CVE-2013-2452 | CVE-2013-2459 | CVE-2013-2466 | CVE-2013-2472 |
| CVE-2013-2412                                       | CVE-2013-2446 | CVE-2013-2453 | CVE-2013-2461 | CVE-2013-2467 | CVE-2013-2473 |
| CVE-2013-2437                                       | CVE-2013-2447 | CVE-2013-2454 | CVE-2013-2462 | CVE-2013-2468 | CVE-2013-3743 |
| CVE-2013-2442                                       | CVE-2013-2448 | CVE-2013-2455 | CVE-2013-2463 | CVE-2013-2469 |               |

**Note:** Xerox® recommends that customers evaluate their security needs periodically and if they need Security patches to address the above CVE issues, schedule an activity with their Xerox Service team to install this announced Security Patch Cluster. Alternatively, the customer can install the Security Patch Cluster using the Update Manager UI from the Xerox® FreeFlow® Print Server Platform.

## 2.0 Applicability

The customer can schedule a Xerox Service or Analyst representative to deliver and install the Security Patch Cluster from the hard disk on the FreeFlow® Print Server. A customer can only perform the install procedures with approval of the Xerox CSE/Analyst. As a result of the very large file size of these deliverables, the download and install of the Solaris 11.3 OS upgrade and October 2017 Security Patch Cluster are not supported from the Update Manager UI on the FreeFlow® Print Server platform.

The Xerox Customer Service Engineer (CSE)/Analyst uses a tool (accessible from a secure FTP site) that enables identification of the currently installed FreeFlow® Print Server software release, Security Patch Cluster, and Java Software version. Run this tool after the Security Patch Cluster install to validate a successful install. Example output from this script for the FreeFlow® Print Server v7 software release and Xerox® Color 1000i Press is as follows:

|                      |                         |
|----------------------|-------------------------|
| FFPS Release Version | 9.0_SP-3_(93.G4.74B.86) |
| FFPS Patch Cluster   | October 2017            |
| Java Version         | Java 7 Update 161       |

The October 2017 Security Patch Cluster is available for the FreeFlow® Print Server v9 release running on the Xerox® printer products below:

1. Xerox® Color 800i/1000i Press
2. Xerox® Versant® 3100 Press

## 3.0 Patch Install

Xerox® strives to deliver these critical Security patch updates in a timely manner. The customer process to obtain Security Patch Cluster updates (delivered on a quarterly basis) is to contact the Xerox hotline support number. Xerox Service or an analyst can install the Patch Cluster using a script utility that will support installing the Security Patch Cluster from the hard disk on the FreeFlow® Print Server platform.

The Security Patch Cluster deliverables are available on a secure FTP site once they are ready for customer delivery. The Xerox CSE/Analyst can download and prepare for the install by writing the Solaris 11.3 OS Upgrade and/or the Security Patch Cluster into a known directory location on the FreeFlow® Print Server platform.

The FreeFlow® Print Server is on top of the Solaris 11.2 OS for the Color 800i/1000i Press. Upgrade to the Solaris 11.3 OS is required prior to installing the October 2017 Security Patch Cluster. Delivery of the Solaris 11.3 OS upgrade includes ZIP files as part 1 and part 2 to address file size issues. Once the patch cluster has been prepared on the hard disk, a script is run to perform the install.

Delivery of the Security Patch Cluster includes ZIP files separated as part 1 and part 2 to address file size issues. Once the patch cluster has been prepared on the hard disk, a script is run to perform the install. Make sure that the Color 800i/1000i Press is upgraded to the Solaris 11.3OS prior to installing the October 2017 Security Patch Cluster.

**Note:** The install of this Security Patch Cluster and/or Solaris 11 OS upgrade can fail if the archive file containing the software is corrupted from when downloading the deliverables from the SFTP site, or uploading them to the FreeFlow® Print Server platform over a network connection. The table below illustrate Solaris checksums and file size on Windows for the Solaris 11.3OS upgrade files.

### Solaris 11.3 OS Upgrade Files (for Xerox® Color 800i/1000i Press only)

| Security Patch File         | Windows Size (Kb) | Solaris Size (bytes) | Solaris Checksum |
|-----------------------------|-------------------|----------------------|------------------|
| Sol-11.3_Upgrade_Part-1.zip | 4,727,677         | 4,841,140,675        | 41735 9455353    |
| Sol-11.3_Upgrade_Part-2.zip | 3,504,985         | 3,589,103,767        | 56371 7009969    |

Verify integrity of the Solaris 11.3 ZIP files contained on the FreeFlow® Print Server hard drive by comparing it to the original archive file size checksum with the actual checksum of these files on the platform. Change directory to the location of the Solaris 11.3 ZIP files and use the UNIX 'sum' command to output the check sum numbers of each ZIP file (E.g., 'sum sum Sol-11.3\_Upgrade\_Part-1.zip'). The output of the 'sum' command should match the above table.

The table below illustrate Solaris checksums and file size on Windows for the Security Patch Cluster files.

### October 2017 Security Patch Cluster Files

| Security Patch File                             | Windows Size (Kb) | Solaris Size (bytes) | Solaris Checksum |
|---|-------------------|----------------------|------------------|
| Oct2017AndJava7Update161Patches_v9S11-Part1.zip | 3,507,847         | 3,592,034,640        | 59474 7015693    |
| Oct2017AndJava7Update161Patches_v9S11-Part2.zip | 3,602,804         | 3,689,270,801        | 12242 7205608    |

Verify integrity of the Security Patch ZIP files contained on the FreeFlow® Print Server hard drive by comparing it to the original archive file size checksum with the actual checksum of these files on the platform. Change directory to the location of the Security Patch Cluster ZIP files and use the UNIX 'sum' command to output the check sum numbers of each ZIP file (E.g., 'sum Oct2017AndJava7Update161Patches\_v9S11-Part1.zip'). The output of the 'sum' command should match the above table.



## 4.0 Disclaimer

The information provided in this Xerox® Product Response is provided "as is" without warranty of any kind. Xerox® Corporation disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Xerox® Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this Xerox® Product Response including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox® Corporation has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.

