



Alert – End-of-Support (EOS) Software (Adobe, Cisco, Microsoft...): January 2019 – April 2020

Description:

The importance of replacing software before its End-of-Support (EOS) is critical. EOS occurs when software updates, patches, and other forms of support are no longer offered, resulting in software becoming prone to future security vulnerabilities.

Using unsupported software and firmware/hardware, puts organizations at risk in the following ways:

- Subsequent vulnerabilities disclosures place your organization at significant risk.
- Subject your organization to regulatory compliance issues/violations.
- Increases support costs by having a need for extended support

The process of finding EOS dates and locating all the instances of obsolete products can be a difficult and time-consuming task. The following table is for software with EOS dates in the next 12 months and please take a look and check if one or many of your softwares, hardwares or firmwares are not among the End-of-Support (EOS) list below and then react:

| Product Name | Product Name | Product Name | Product Name | Product Name |
|--|--------------|------------------|--------------|------------------------------|
| ColdFusion | Adobe | 11.x, 2016, 2018 | 11.X | 4/30/2019 (for core support) |
| ColdFusion | Adobe | 11.x, 2016, 2018 | 10.x | 5/16/2019 (extended Support) |
| LiveCycle Correspondence Management Solution | Adobe | | 10.x.x | 3/31/19 |
| LiveCycle Designer ES3 | Adobe | | 10.x.x | 3/31/19 |
| LiveCycle Digital Signatures ES3 | Adobe | | 10.x.x | 3/31/19 |
| LiveCycle ES3 Connector for EMC Documentum | Adobe | | 10.x.x | 3/31/19 |
| LiveCycle ES3 Connector for IBM Content Manager | Adobe | | 10.x.x | 3/31/19 |
| LiveCycle ES3 Connector for IBM FileNet | Adobe | | 10.x.x | 3/31/19 |
| LiveCycle ES3 Connector for Microsoft SharePoint | Adobe | | 10.x.x | 3/31/19 |
| LiveCycle Forms ES3 | Adobe | | 10.x.x | 3/31/19 |
| LiveCycle Output ES3 | Adobe | | 10.x.x | 3/31/19 |

| | | | | |
|----------------------------------|------------|----------------------|---|--|
| LiveCycle Process Management ES3 | Adobe | | 10.x.x | 3/31/19 |
| LiveCycle Reader Extensions ES3 | Adobe | | 10.x.x | 3/31/19 |
| LiveCycle Rights Management ES3 | Adobe | | 10.x.x | 3/31/19 |
| LiveCycle Workbench ES3 | Adobe | | 10.x.x | 3/31/19 |
| Apache Struts | Apache | 2.5.18 GA, 2.3.36 GA | 2.3.X | 5/14/19 |
| Bitbucket Server | Atlassian | 4.12-5.16 | 4.13, 4.14, 5.0, 5.1 | 1/20/2019, 2/21/2019, 5/02/2019, 6/06/2019 |
| Confluence | Atlassian | 6.1-6.12 | 6.1, 6.2 | 3/20/2019, 5/15/2019 |
| Jira Core | Atlassian | 7.3-7.12 | 7.3, 7.4 | 1/032019, 6/29/2019 |
| Jira Service Desk | Atlassian | 3.3-3.15 | 3.3, 3.4, 3.5, 3.6 | 1/03/2019, 3/142019, 4/27/2019, 6/29/2019 |
| Jira Software | Atlassian | 7.3-7.12 | 7.3, 7.4 | 1/03/2019, 6/29/2019 |
| Checkpoint Endpoint Security | Checkpoint | | E80.6x (except for E80.62, E80.64), EP5.6 | 11/01/2018, 6/012019 |
| WebEx Meetings Server | Cisco | 2.8 | 2.8 | 4/20/2019 |

| | | | | |
|--|------------|---|-------------------|----------------------|
| WebEx Meetings Suite | Cisco | | 32.12.x, 32.xx | 1/11/2019, 5/24/2019 |
| Websense / Forcepoint URL Filtering | Forcepoint | 7.0, 7.1, 7.5, 7.6, 7.7, 7.7.3, 7.8.1, 7.8.2, 7.8.3, 7.8.4, 8.0, 8.0.1, 8.1, 8.2, 8.3, 8.4, 8.5 | 7.0, 7.1, 7.5 | 4/02/2019 |
| Websense Express | Forcepoint | 1.0.0 | 1.0.0 | 3/31/19 |
| JBoss Web Server Version 1.x | | | | 4/1/20 |
| Joomla | Joomla | 3.8.13 | | 1/15/19 |
| Mediawiki | Mediawiki | | 1.27.x (LTS) | 6/012019 |
| Exchange Server 2010 | Microsoft | | | 1/14/20 |
| Internet Information Service (IIS) | Microsoft | | 7.5 | 1/4/20 |
| Windows Server 2008 and 2008 R2 | Microsoft | | | 1/14/20 |
| Microsoft Windows 7 | Microsoft | | | 1/14/20 |
| Windows 10 ,version 1803 (Home,Pro, Pro workstations) | Microsoft | | | 11/12/19 |
| Windows 10, version 1607 (Enterprise and Education Editions) | Microsoft | | | 4/9/19 |
| Windows 10, version 1703 (Enterprise and Education Editions) | Microsoft | | | 10/8/19 |

| | | | | |
|--|--------------|---------|-----------------------------|--|
| Windows 10, version 1703 (Home,Pro, Pro workstations) | Microsoft | | | 10/9/2019 |
| Windows 10, version 1709 (Home,Pro, Pro workstations) | Microsoft | | | 4/9/19 |
| Microsoft Windows 10, version 1709 (Enterprise and Education Editions) | Microsoft | | | 4/14/20 |
| Microsoft Windows 10, version 1809 (Home,Pro, Pro workstations) | Microsoft | | | 4/14/20 |
| Nginx Version 1.12 Stable | Nginx | current | 1.10, 1.11 | |
| Nginx Version 1.13 MainLine | Nginx | current | 1.10, 1.11 | |
| syslog-ng Premium | One Identity | 7.0.11 | 1.0.1, 7.0.8, 7.0.9, 7.0.10 | 2/25/2019, 4/22/2019, 6/19/2019, 8/19/2019 |
| OpenSSL | OpenSSL | 1.1.0 | 1.0.2 | 12/31/19 |
| Pearl 5.26.0 | Perl | | 5.22 and under | |
| PHP Version 7.1 | PHP | | | 12/1/19 |
| Phusion Passenger | Phusion | 5.3.5 | | |
| Python 2.7 | Python | | | 1/20/20 |

| | | | | |
|----------------------------|------------|--|---|-----------|
| TippingPoint IPS | TrendMirco | | (3.7.0 N-Platform, 3.7.1-3.7.2 N/NX-Platform, 3.8.0 N/NX-Platform, 3.8.1 N/NX-Platform, 3.8.2 N/NX-Platform, 3.8.3 N/NX-Platform, 3.9.0 N/NX-Platform, 3.9.1 N/NX-Platform), 3.8.4 N/NX-Platform, | 2/28/2019 |
| TippingPoint IPS Appliance | TrendMirco | | JC021A (2500N), JC022A (5100N), JC577A (6100N) | 1/31/2019 |

| | | | | |
|---------------------------------------|------------|--|---|-----------|
| TippingPoint Miscellaneous Devices | TrendMirco | | JC007A (TippingPoint Smart ZPHA 10G Multi- Mode Module), JC008A (TippingPoint Smart ZPHA 10G Single- Mode Module), JC010A (TippingPoint 10G XFP LR Transceiver), JC011A (TippingPoint 10G XFP SR Transceiver), JC182A (Core Controller) | 6/30/2019 |
| TippingPoint NextGen Firewall | TrendMirco | | 1.0.x, 1.1.0, 1.1.1, 1.2.1, 1.2.2, 1.2.3 | 1/31/2019 |

| | | | | |
|---|------------|--|---|---------------------------------|
| TippingPoint NextGen Firewall Appliance | TrendMicro | | JC850A (S1050F), JC851A (S3010F), JC852A (S3020F), JC853A (S8005F), JC854A (S8010F) | 1/31/2019 |
| TippingPoint Security Management System | Tripwire | | 4.5.0, 4.6.0, 5.0.0 | 2/28/2019, 2/28/2019, 2/28/2019 |
| TippingPoint Threat Protection System | Tripwire | | (4.0.0, 4.0.2, 4.1.0, 4.1.1, 4.1.2, 4.2.0), 5.0.0 | 2/28/19 |
| Tripwire Configuration Compliance Manager | Tripwire | | 5.17.3, 5.17.4, 5.17.5 | 1/01/2019, 4/01/2019, 6/01/2019 |
| Tripwire Connect | Tripwire | | 3.5 | 5/1/19 |

| | | | | |
|--------------------------------------|----------|---------|----------------------|---|
| Tripwire Enterprise | Tripwire | 8.7 | 8.5.3, 8.5.4 | 3/01/2019, 6/01/2019 |
| Tripwire IP360 | Tripwire | | 8.1.1 | 5/01/2019 |
| Tripwire Log Center | Tripwire | | 7.2.4, 7.2.5 | 3/01/2019, 6/01/2019 |
| Tripwire Security Intelligence Hub | Tripwire | | 2.7.3 | 3/1/19 |
| Ubuntu | Ubuntu | | 14.04 LTS | 4/01/2019 |
| VMware Fusion | VMWare | 10, 11 | 10 | 3/26/2019 |
| VMware Horizon View | VMWare | | 6.x | 6/19/2019 |
| VMware vSphere Data Protection (VDP) | VMWare | current | 6.5 | 6.5 and until end of active Support and Subscription (SnS) agreement, |
| VMware Workstation | VMWare | | 14 Pro and 14 Player | 3/26/2019 |
| Corel WinZip | Winzip | | 20 | 4/30/19 |

Solutions (Mitigations):

Rw-CSIRT is strongly recommending **users** and **administrators** to check all the software and firmware/hardware that are currently in use in your institutions, if they are not listed above and then replace/upgrade them before it reaches EOS and this will significantly reduce any risks and costs associated with EOS

Any assistance: please contact Rw-CSIRT by calling us on [4045](tel:4045) or writing to security@risa.rw

References: <https://www.cisecurity.org/wp-content/uploads/2019/03/EOS-table.pdf>

National Computer Security and Incident Response Team (Rw-CSIRT) Mission

Rw-CSIRT mission is to build cyber-security capabilities to increase the capacity of “early **Detection**, **Prevention**, **Response** to incidents and **Reduce** Vulnerability” and raise cyber security awareness in public.