## Adobe Acrobat Reader DC

|  |  |  |  |
| --- | --- | --- | --- |
| Идентификатор CVE | Идентификатор ФСТЭК | Описание уязвимостей | Уровень опасности уязвимости |
| CVE-2021-40731 | BDU:2021-05074 | Adobe Acrobat Reader DC version 21.007.20095 (and earlier), 21.007.20096 (and earlier), 20.004.30015 (and earlier), and 17.011.30202 (and earlier) is affected by an out-of-bounds write vulnerability when parsing a crafted JPEG2000 file, which could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2021-40730 | BDU:2021-05073 | Adobe Acrobat Reader DC version 21.007.20095 (and earlier), 21.007.20096 (and earlier), 20.004.30015 (and earlier), and 17.011.30202 (and earlier) is affected by a use-after-free that allow a remote attacker to disclose sensitive information on affected installations of of Adobe Acrobat Reader DC. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPG2000 images. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.3) |
| CVE-2021-40729 | BDU:2021-05072 | Adobe Acrobat Reader DC version 21.007.20095 (and earlier), 21.007.20096 (and earlier), 20.004.30015 (and earlier), and 17.011.30202 (and earlier) is affected by a out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious PDF file. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.3) |
| CVE-2021-40728 | BDU:2021-05071 | Adobe Acrobat Reader DC version 21.007.20095 (and earlier), 21.007.20096 (and earlier), 20.004.30015 (and earlier), and 17.011.30202 (and earlier) is affected by a use-after-free vulnerability in the processing of the GetURL function on a global object window that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2021-39857 | BDU:2021-05071 | Adobe Acrobat Reader DC add-on for Internet Explorer versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to check for existence of local files. Exploitation of this issue requires user interaction in that a victim must visit an attacker controlled web page. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.3) |
| CVE-2020-24439 | BDU:2020-05587 | Acrobat Reader DC for macOS versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a security feature bypass. While the practical security impact is minimal, a defense-in-depth fix has been implemented to further harden the Adobe Reader update process. | Низкий уровень опасности (базовая оценка CVSS 2.0 составляет 1.2) |
| CVE-2020-24433 | BDU:2020-05602 | Adobe Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a local privilege escalation vulnerability that could enable a user without administrator privileges to delete arbitrary files and potentially execute arbitrary code as SYSTEM. Exploitation of this issue requires an attacker to socially engineer a victim, or the attacker must already have some access to the environment. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9.3) |
| CVE-2020-24432 | BDU:2020-05589 | Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) and Adobe Acrobat Pro DC 2017.011.30175 (and earlier) are affected by an improper input validation vulnerability that could result in arbitrary JavaScript execution in the context of the current user. To exploit this issue, an attacker must acquire and then modify a certified PDF document that is trusted by the victim. The attacker then needs to convince the victim to open the document. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2020-24431 | BDU:2020-05589 | Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) for macOS are affected by a security feature bypass that could result in dynamic library code injection by the Adobe Reader process. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.8) |
| CVE-2016-7854 | Отсутствует | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, CVE-2016-7019, CVE-2016-7852, and CVE-2016-7853. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7853 | Отсутствует | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, CVE-2016-7019, CVE-2016-7852, and CVE-2016-7854. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7852 | Отсутствует | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, CVE-2016-7019, CVE-2016-7853, and CVE-2016-7854. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7019 | BDU:2016-02244 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, and CVE-2016-7018. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7018 | BDU:2016-02245 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7017 | BDU:2016-02246 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7016 | BDU:2016-02247 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7015 | BDU:2016-02248 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7014 | BDU:2016-02248 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7013 | BDU:2016-02250 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7012 | BDU:2016-02251 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7011 | BDU:2016-02252 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7010 | BDU:2016-02253 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7009 | BDU:2016-02254 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7008 | BDU:2016-02255 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7007 | BDU:2016-02256 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7006 | BDU:2016-02257 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7005 | BDU:2016-02258 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7004 | BDU:2016-02259 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7003 | BDU:2016-02259 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7002 | BDU:2016-02261 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7001 | BDU:2016-02262 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-7000 | BDU:2016-02263 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6999 | BDU:2016-02264 | Integer overflow in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6998 | BDU:2016-02265 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6997 | BDU:2016-02266 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6996 | BDU:2016-02267 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6995 | BDU:2016-02268 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6994 | BDU:2016-02269 | Heap-based buffer overflow in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-6939. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6993 | BDU:2016-02270 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, and CVE-2016-6988. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6988 | BDU:2016-02271 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6979 | BDU:2016-02271 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6978 | BDU:2016-02273 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6977 | BDU:2016-02274 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6976 | BDU:2016-02275 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6975 | BDU:2016-02276 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6974 | BDU:2016-02277 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6973 | BDU:2016-02278 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6972 | BDU:2016-02279 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6971 | BDU:2016-02280 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6970 | BDU:2016-02281 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6969 | BDU:2016-02282 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6968 | BDU:2016-02283 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6967 | BDU:2016-02284 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6966 | BDU:2016-02285 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6965 | BDU:2016-02286 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6964 | BDU:2016-02287 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6963 | BDU:2016-02288 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6962 | BDU:2016-02289 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6961 | BDU:2016-02290 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6960 | BDU:2016-02291 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6959 | BDU:2016-02292 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6958 | BDU:2016-02293 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to bypass intended access restrictions via unspecified vectors. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6957 | BDU:2016-02294 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6956 | BDU:2016-02294 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6955 | BDU:2016-02296 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6954 | BDU:2016-02297 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6953 | BDU:2016-02298 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6952 | BDU:2016-02299 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6951 | BDU:2016-02299 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6950 | BDU:2016-02300 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6949 | BDU:2016-02301 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6948 | BDU:2016-02301 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6947 | BDU:2016-02303 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6946 | BDU:2016-02303 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6945 | BDU:2016-02303 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6944 | BDU:2016-02305 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6943 | Отсутствует | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6942 | BDU:2016-02305 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6941 | BDU:2016-02305 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6940 | BDU:2016-02305 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6939 | BDU:2016-02305 | Heap-based buffer overflow in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-6994. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6938 | Отсутствует | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4255. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-6937 | Отсутствует | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4265, CVE-2016-4266, CVE-2016-4267, CVE-2016-4268, CVE-2016-4269, and CVE-2016-4270. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4270 | BDU:2016-02307 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4265, CVE-2016-4266, CVE-2016-4267, CVE-2016-4268, and CVE-2016-4269. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4269 | BDU:2016-02307 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4265, CVE-2016-4266, CVE-2016-4267, CVE-2016-4268, and CVE-2016-4270. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4268 | Отсутствует | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4265, CVE-2016-4266, CVE-2016-4267, CVE-2016-4269, and CVE-2016-4270. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4267 | BDU:2016-02307 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4265, CVE-2016-4266, CVE-2016-4268, CVE-2016-4269, and CVE-2016-4270. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4266 | BDU:2016-02307 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4265, CVE-2016-4267, CVE-2016-4268, CVE-2016-4269, and CVE-2016-4270. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4265 | BDU:2016-02078 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4266, CVE-2016-4267, CVE-2016-4268, CVE-2016-4269, and CVE-2016-4270. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4255 | BDU:2016-01775 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2016-4254 | BDU:2016-01775 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, and CVE-2016-4252. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4252 | BDU:2016-01777 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4251 | BDU:2016-01778 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4252, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4250 | BDU:2016-01779 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4215 | BDU:2016-01790 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4214 | BDU:2016-01791 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4213 | BDU:2016-01792 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4212 | BDU:2016-01792 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4211 | BDU:2016-01794 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4210 | BDU:2016-01795 | Integer overflow in Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4209 | BDU:2016-01796 | Heap-based buffer overflow in Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4208 | BDU:2016-01797 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4207 | BDU:2016-01798 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4206 | BDU:2016-01799 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4205 | BDU:2016-01800 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4204 | BDU:2016-01801 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4203 | BDU:2016-01802 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4202 | BDU:2016-01803 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2016-4201 | BDU:2016-01804 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4200 | BDU:2016-01805 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2016-4199 | BDU:2016-01806 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2016-4198 | BDU:2016-01807 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2016-4197 | BDU:2016-01808 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2016-4196 | BDU:2016-01809 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2016-4195 | BDU:2016-01810 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2016-4194 | BDU:2016-01811 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4193 | BDU:2016-01812 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4192 | BDU:2016-01813 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4191 | BDU:2016-01814 | Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4119 | BDU:2016-02080 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4107 | BDU:2016-01180 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, and CVE-2016-4102. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4106 | BDU:2016-01286 | Untrusted search path vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows local users to gain privileges via a Trojan horse resource in an unspecified directory, a different vulnerability than CVE-2016-1087 and CVE-2016-1090. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7.2) |
| CVE-2016-4105 | BDU:2016-01181 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, and CVE-2016-4104. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4104 | BDU:2016-01182 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4103 | BDU:2016-01182 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4102 | BDU:2016-01184 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4101 | BDU:2016-01185 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4100 | BDU:2016-01185 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4099 | BDU:2016-01187 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4098 | BDU:2016-01188 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4097 | BDU:2016-01189 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4096 | BDU:2016-01190 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4095 | BDU:2017-01275 | Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4094 | BDU:2016-01191 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4093 | BDU:2016-01192 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4092 | BDU:2016-01287 | Heap-based buffer overflow in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4091. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4091 | BDU:2016-01287 | Heap-based buffer overflow in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4092. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4090 | BDU:2016-01193 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4089 | BDU:2016-01194 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-4088 | BDU:2016-01195 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1130 | BDU:2016-01210 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1129 | BDU:2016-01211 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1128 | BDU:2016-01212 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1127 | BDU:2016-01213 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1126 | BDU:2016-01214 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1125 | BDU:2016-01215 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1124 | BDU:2016-01216 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1123 | BDU:2016-01217 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1122 | BDU:2016-01218 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1121 | BDU:2016-01219 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1120 | BDU:2016-01220 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1119 | BDU:2016-01221 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1118 | BDU:2016-01222 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1117 | BDU:2016-01290 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1039, CVE-2016-1040, CVE-2016-1041, CVE-2016-1042, CVE-2016-1044, and CVE-2016-1062. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1116 | BDU:2016-01223 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1112 | BDU:2016-01294 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to obtain sensitive information via unspecified vectors. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1111 | BDU:2016-01224 | Double free vulnerability in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code via a crafted Graphics State dictionary. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2016-1095 | BDU:2016-01224 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1094 | BDU:2016-01225 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1093 | BDU:2016-01227 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1092 | BDU:2016-01310 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to obtain sensitive information from process memory via unspecified vectors, a different vulnerability than CVE-2016-1079. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.0) |
| CVE-2016-1091 | BDU:2017-01278 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1090 | BDU:2016-01311 | Untrusted search path vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows local users to gain privileges via a Trojan horse resource in an unspecified directory, a different vulnerability than CVE-2016-1087 and CVE-2016-4106. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7.2) |
| CVE-2016-1089 | BDU:2017-01279 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1088 | BDU:2017-01279 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1087 | Отсутствует | Untrusted search path vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows local users to gain privileges via a Trojan horse resource in an unspecified directory, a different vulnerability than CVE-2016-1090 and CVE-2016-4106. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7.2) |
| CVE-2016-1086 | Отсутствует | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1085 | Отсутствует | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1084 | BDU:2016-01231 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1083 | BDU:2016-01231 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1082 | BDU:2016-01233 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1081 | BDU:2016-01233 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1080 | BDU:2016-01235 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1079 | BDU:2016-01313 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to obtain sensitive information from process memory via unspecified vectors, a different vulnerability than CVE-2016-1092. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.0) |
| CVE-2016-1078 | BDU:2016-01236 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1077 | BDU:2016-01237 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1076 | BDU:2016-01238 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1075 | BDU:2016-01239 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1074 | BDU:2016-01240 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1073 | BDU:2016-01241 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1072 | BDU:2016-01242 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1071 | BDU:2016-01243 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1070 | BDU:2016-01244 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1069 | BDU:2016-01245 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1068 | BDU:2016-01246 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1067 | BDU:2016-01247 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1066 | BDU:2016-01248 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1065 | BDU:2016-01249 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1064 | BDU:2016-01250 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1063 | BDU:2016-01251 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1062 | BDU:2016-01314 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1039, CVE-2016-1040, CVE-2016-1041, CVE-2016-1042, CVE-2016-1044, and CVE-2016-1117. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1061 | BDU:2016-01252 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1060 | BDU:2016-01253 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1059 | BDU:2016-01254 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1058 | BDU:2016-01255 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1057 | BDU:2016-01256 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1056 | BDU:2016-01257 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1055 | BDU:2016-01258 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1054 | BDU:2016-01259 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1053 | BDU:2016-01260 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1052 | BDU:2016-01261 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1051 | BDU:2016-01262 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1050 | BDU:2016-01262 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1049 | BDU:2016-01263 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1048 | BDU:2016-01265 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1047 | BDU:2016-01265 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1046 | BDU:2016-01266 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1045 | BDU:2016-01268 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1044 | BDU:2016-01269 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1039, CVE-2016-1040, CVE-2016-1041, CVE-2016-1042, CVE-2016-1062, and CVE-2016-1117. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1043 | BDU:2016-01315 | Integer overflow in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1042 | BDU:2016-01270 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1039, CVE-2016-1040, CVE-2016-1041, CVE-2016-1044, CVE-2016-1062, and CVE-2016-1117. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1041 | BDU:2016-01271 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1039, CVE-2016-1040, CVE-2016-1042, CVE-2016-1044, CVE-2016-1062, and CVE-2016-1117. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1040 | BDU:2016-01272 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1039, CVE-2016-1041, CVE-2016-1042, CVE-2016-1044, CVE-2016-1062, and CVE-2016-1117. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1039 | BDU:2016-01273 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1040, CVE-2016-1041, CVE-2016-1042, CVE-2016-1044, CVE-2016-1062, and CVE-2016-1117. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1038 | BDU:2016-01274 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1039, CVE-2016-1040, CVE-2016-1041, CVE-2016-1042, CVE-2016-1044, CVE-2016-1062, and CVE-2016-1117. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1037 | BDU:2016-01275 | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1009 | BDU:2016-00779 | Adobe Reader and Acrobat before 11.0.15, Acrobat and Acrobat Reader DC Classic before 15.006.30121, and Acrobat and Acrobat Reader DC Continuous before 15.010.20060 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1007. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-1008 | BDU:2016-00780 | Untrusted search path vulnerability in Adobe Reader and Acrobat before 11.0.15, Acrobat and Acrobat Reader DC Classic before 15.006.30121, and Acrobat and Acrobat Reader DC Continuous before 15.010.20060 on Windows and OS X allows local users to gain privileges via a Trojan horse DLL in an unspecified directory. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7.2) |
| CVE-2016-1007 | BDU:2016-00781 | Adobe Reader and Acrobat before 11.0.15, Acrobat and Acrobat Reader DC Classic before 15.006.30121, and Acrobat and Acrobat Reader DC Continuous before 15.010.20060 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1009. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-0947 | BDU:2016-00086 | Untrusted search path vulnerability in Adobe Download Manager, as used in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X, allows local users to gain privileges via a crafted resource in an unspecified directory. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7.2) |
| CVE-2016-0946 | BDU:2016-00086 | Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, and CVE-2016-0945. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-0945 | BDU:2016-00088 | Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, and CVE-2016-0946. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-0944 | BDU:2016-00088 | Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0945, and CVE-2016-0946. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-0943 | BDU:2016-00090 | Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X mishandle the Global object, which allows attackers to bypass JavaScript API execution restrictions via unspecified vectors. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2016-0942 | BDU:2016-00091 | Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0944, CVE-2016-0945, and CVE-2016-0946. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-0941 | BDU:2016-00092 | Use-after-free vulnerability in the Search object implementation in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0932, CVE-2016-0934, CVE-2016-0937, and CVE-2016-0940. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2016-0940 | BDU:2016-00092 | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0932, CVE-2016-0934, CVE-2016-0937, and CVE-2016-0941. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-0939 | BDU:2016-00094 | Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (uninitialized pointer dereference and memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0942, CVE-2016-0944, CVE-2016-0945, and CVE-2016-0946. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2016-0938 | BDU:2016-00094 | The AcroForm plugin in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, CVE-2016-0945, and CVE-2016-0946. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9.3) |
| CVE-2016-0937 | BDU:2016-00096 | Use-after-free vulnerability in the OCG object implementation in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0932, CVE-2016-0934, CVE-2016-0940, and CVE-2016-0941. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9.3) |
| CVE-2016-0936 | BDU:2016-00097 | Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted JPEG 2000 data, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, CVE-2016-0945, and CVE-2016-0946. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9.3) |
| CVE-2016-0935 | BDU:2016-00097 | Double free vulnerability in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code via a crafted ExtGState dictionary. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2016-0934 | BDU:2016-00099 | Use-after-free vulnerability in AGM.dll in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code via a multiple-layer PDF document, a different vulnerability than CVE-2016-0932, CVE-2016-0937, CVE-2016-0940, and CVE-2016-0941. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2016-0933 | BDU:2016-00100 | Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, CVE-2016-0945, and CVE-2016-0946. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-0932 | BDU:2016-00101 | Use-after-free vulnerability in the Doc object implementation in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0934, CVE-2016-0937, CVE-2016-0940, and CVE-2016-0941. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2016-0931 | BDU:2016-00102 | Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted FileAttachment annotation, a different vulnerability than CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, CVE-2016-0945, and CVE-2016-0946. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-8458 | BDU:2016-00392 | Heap-based buffer overflow in AGM.dll in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to execute arbitrary code via a multiple-layer PDF document, a different vulnerability than CVE-2015-6696 and CVE-2015-6698. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-7829 | BDU:2015-11798 | Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows mishandle junctions in the Synchronizer directory, which allows attackers to delete arbitrary files via Adobe Collaboration Sync, a related issue to CVE-2015-2428. | Низкий уровень опасности (базовая оценка CVSS 2.0 составляет 1.9) |
| CVE-2015-7650 | BDU:2015-11979 | Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via a crafted CMAP table in a PDF document, a different vulnerability than CVE-2015-6685, CVE-2015-6686, CVE-2015-6693, CVE-2015-6694, CVE-2015-6695, and CVE-2015-7622. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-7624 | BDU:2015-11778 | Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allow attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2015-5583, CVE-2015-6705, and CVE-2015-6706. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.0) |
| CVE-2015-7623 | BDU:2015-11777 | The ANAuthenticateResource method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, and CVE-2015-7620. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-7622 | BDU:2015-11777 | Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-6685, CVE-2015-6686, CVE-2015-6693, CVE-2015-6694, and CVE-2015-6695. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-7621 | BDU:2015-11775 | Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to execute arbitrary code via a crafted U3D object, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-7615, and CVE-2015-7617. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-7620 | BDU:2015-11775 | The ANSendForBrowserReview method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-7619 | BDU:2015-11773 | The ANShareFile2 method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-7618 | BDU:2015-11772 | The CBAutoConfigCommentRepository method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-7617 | BDU:2015-11771 | Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to execute arbitrary code by leveraging improper EScript exception handling, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-7615, and CVE-2015-7621. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-7616 | BDU:2015-11770 | The ANVerifyComments method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-7615 | BDU:2015-11769 | Use-after-free vulnerability in a SaveAs feature in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-7617, and CVE-2015-7621. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-7614 | BDU:2015-11768 | Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions and execute arbitrary commands via an app.launchURL call, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6725 | BDU:2015-11758 | The ANSendForSharedReview method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6724 | BDU:2015-11757 | The ANSendForApproval method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6723 | BDU:2015-11756 | The ANTrustPropagateAll method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6722 | BDU:2015-11756 | The CBSharedReviewStatusDialog method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6721 | BDU:2015-11754 | The CBSharedReviewSecurityDialog method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6720 | BDU:2015-11753 | The ANRunSharedReviewEmailStep method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6719 | BDU:2015-11752 | The CBSharedReviewCloseDialog method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6718 | BDU:2015-11751 | The CBSharedReviewIfOfflineDialog method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6717 | BDU:2015-11750 | The DynamicAnnotStore method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6716 | BDU:2015-11749 | The ANSendForFormDistribution method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6715 | BDU:2015-11748 | The Function apply implementation in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6714 | BDU:2015-11748 | The Function bind implementation in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6713 | BDU:2015-11746 | The Function call implementation in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7.5) |
| CVE-2015-6712 | BDU:2015-11746 | The ANSendApprovalToAuthorEnabled method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6711 | BDU:2015-11744 | The DoIdentityDialog method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6710 | BDU:2015-11743 | The CBBBRInit method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6709 | BDU:2015-11742 | The CBBBRInvite method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6708 | BDU:2015-11741 | The ANStartApproval method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6707 | BDU:2015-11740 | The ANSendForReview method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6706 | BDU:2015-11740 | Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allow attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2015-5583, CVE-2015-6705, and CVE-2015-7624. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.0) |
| CVE-2015-6705 | BDU:2015-11738 | Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allow attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2015-5583, CVE-2015-6706, and CVE-2015-7624. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.0) |
| CVE-2015-6704 | BDU:2015-11737 | The animations property implementation in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to obtain sensitive information from process memory via a function call, a different vulnerability than CVE-2015-6697, CVE-2015-6699, CVE-2015-6700, CVE-2015-6701, CVE-2015-6702, and CVE-2015-6703. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.3) |
| CVE-2015-6703 | BDU:2015-11736 | The loadFlashMovie function in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to obtain sensitive information from process memory via invalid arguments, a different vulnerability than CVE-2015-6697, CVE-2015-6699, CVE-2015-6700, CVE-2015-6701, CVE-2015-6702, and CVE-2015-6704. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.3) |
| CVE-2015-6702 | BDU:2015-11735 | The createSquareMesh function in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to obtain sensitive information from process memory via invalid arguments, a different vulnerability than CVE-2015-6697, CVE-2015-6699, CVE-2015-6700, CVE-2015-6701, CVE-2015-6703, and CVE-2015-6704. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.3) |
| CVE-2015-6701 | BDU:2015-11734 | The ambientIlluminationColor property implementation in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to obtain sensitive information from process memory via a function call, a different vulnerability than CVE-2015-6697, CVE-2015-6699, CVE-2015-6700, CVE-2015-6702, CVE-2015-6703, and CVE-2015-6704. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.3) |
| CVE-2015-6700 | BDU:2015-11733 | The setBackground function in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to obtain sensitive information from process memory via invalid arguments, a different vulnerability than CVE-2015-6697, CVE-2015-6699, CVE-2015-6701, CVE-2015-6702, CVE-2015-6703, and CVE-2015-6704. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.0) |
| CVE-2015-6699 | BDU:2015-11732 | The addForegroundSprite function in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to obtain sensitive information from process memory via invalid arguments, a different vulnerability than CVE-2015-6697, CVE-2015-6700, CVE-2015-6701, CVE-2015-6702, CVE-2015-6703, and CVE-2015-6704. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.3) |
| CVE-2015-6698 | BDU:2015-11731 | Heap-based buffer overflow in the AcroForm implementation in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-6696. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6697 | BDU:2015-11731 | Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allow attackers to obtain sensitive information about color objects from process memory by reading a light object's RGB data, a different vulnerability than CVE-2015-6699, CVE-2015-6700, CVE-2015-6701, CVE-2015-6702, CVE-2015-6703, and CVE-2015-6704. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6696 | BDU:2015-11729 | Heap-based buffer overflow in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-6698. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6695 | BDU:2015-11729 | Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted use of the value attribute, a different vulnerability than CVE-2015-6685, CVE-2015-6686, CVE-2015-6693, CVE-2015-6694, and CVE-2015-7622. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6694 | BDU:2015-11727 | Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted use of the fillColor attribute, a different vulnerability than CVE-2015-6685, CVE-2015-6686, CVE-2015-6693, CVE-2015-6695, and CVE-2015-7622. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6693 | BDU:2015-11726 | The signatureSetSeedValue method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted arguments, a different vulnerability than CVE-2015-6685, CVE-2015-6686, CVE-2015-6694, CVE-2015-6695, and CVE-2015-7622. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6692 | BDU:2015-11725 | Buffer overflow in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to obtain sensitive information via unspecified vectors. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.0) |
| CVE-2015-6691 | BDU:2015-11724 | Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-7615, CVE-2015-7617, and CVE-2015-7621. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-6690 | BDU:2015-11723 | Use-after-free vulnerability in the popUpMenuEx method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to execute arbitrary code via crafted arguments, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6691, CVE-2015-7615, CVE-2015-7617, and CVE-2015-7621. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6689 | BDU:2015-11722 | Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to execute arbitrary code via a crafted WillSave document action, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6687, CVE-2015-6688, CVE-2015-6690, CVE-2015-6691, CVE-2015-7615, CVE-2015-7617, and CVE-2015-7621. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6688 | BDU:2015-11722 | Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to execute arbitrary code via a crafted Optional Content Groups (OCG) object in a WillSave document action, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6687, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-7615, CVE-2015-7617, and CVE-2015-7621. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6687 | BDU:2015-11720 | Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-7615, CVE-2015-7617, and CVE-2015-7621. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-6686 | BDU:2015-11719 | Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted set of fields, a different vulnerability than CVE-2015-6685, CVE-2015-6693, CVE-2015-6694, CVE-2015-6695, and CVE-2015-7622. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6685 | BDU:2015-11719 | Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) by using the Format action for unspecified fields, a different vulnerability than CVE-2015-6686, CVE-2015-6693, CVE-2015-6694, CVE-2015-6695, and CVE-2015-7622. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-6684 | BDU:2015-11717 | Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-7615, CVE-2015-7617, and CVE-2015-7621. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-6683 | BDU:2015-11716 | Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5586, CVE-2015-6684, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-7615, CVE-2015-7617, and CVE-2015-7621. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5586 | BDU:2015-11699 | Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-6683, CVE-2015-6684, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-7615, CVE-2015-7617, and CVE-2015-7621. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5583 | BDU:2015-11698 | Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allow attackers to bypass intended sandbox restrictions and obtain sensitive PDF information by launching a print job on a remote printer, a different vulnerability than CVE-2015-6705, CVE-2015-6706, and CVE-2015-7624. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.3) |
| CVE-2015-5115 | BDU:2015-11698 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3095, CVE-2015-5087, CVE-2015-5094, CVE-2015-5100, CVE-2015-5102, CVE-2015-5103, and CVE-2015-5104. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5114 | BDU:2015-10789 | Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-4448, CVE-2015-5095, CVE-2015-5099, CVE-2015-5101, CVE-2015-5111, and CVE-2015-5113. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5113 | BDU:2015-10785 | Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-4448, CVE-2015-5095, CVE-2015-5099, CVE-2015-5101, CVE-2015-5111, and CVE-2015-5114. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-5111 | BDU:2015-10781 | Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-4448, CVE-2015-5095, CVE-2015-5099, CVE-2015-5101, CVE-2015-5113, and CVE-2015-5114. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-5110 | Отсутствует | Stack-based buffer overflow in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-5109 | BDU:2015-10773 | Integer overflow in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5097 and CVE-2015-5108. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-5108 | BDU:2015-10769 | Integer overflow in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5097 and CVE-2015-5109. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5107 | Отсутствует | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to obtain sensitive information via unspecified vectors. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.3) |
| CVE-2015-5106 | BDU:2015-10809 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass intended access restrictions and perform a transition from Low Integrity to Medium Integrity via unspecified vectors, a different vulnerability than CVE-2015-4446 and CVE-2015-5090. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-5105 | BDU:2015-10765 | Heap-based buffer overflow in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5096 and CVE-2015-5098. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5104 | BDU:2015-10761 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3095, CVE-2015-5087, CVE-2015-5094, CVE-2015-5100, CVE-2015-5102, CVE-2015-5103, and CVE-2015-5115. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5103 | BDU:2015-10757 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3095, CVE-2015-5087, CVE-2015-5094, CVE-2015-5100, CVE-2015-5102, CVE-2015-5104, and CVE-2015-5115. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5102 | BDU:2015-10753 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3095, CVE-2015-5087, CVE-2015-5094, CVE-2015-5100, CVE-2015-5103, CVE-2015-5104, and CVE-2015-5115. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5101 | BDU:2015-10749 | Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-4448, CVE-2015-5095, CVE-2015-5099, CVE-2015-5111, CVE-2015-5113, and CVE-2015-5114. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5100 | BDU:2015-10745 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3095, CVE-2015-5087, CVE-2015-5094, CVE-2015-5102, CVE-2015-5103, CVE-2015-5104, and CVE-2015-5115. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5099 | BDU:2015-10741 | Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-4448, CVE-2015-5095, CVE-2015-5101, CVE-2015-5111, CVE-2015-5113, and CVE-2015-5114. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5098 | BDU:2015-10741 | Heap-based buffer overflow in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5096 and CVE-2015-5105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5097 | BDU:2015-10733 | Integer overflow in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5108 and CVE-2015-5109. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5096 | BDU:2015-10729 | Heap-based buffer overflow in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5098 and CVE-2015-5105. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5095 | BDU:2015-10725 | Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-4448, CVE-2015-5099, CVE-2015-5101, CVE-2015-5111, CVE-2015-5113, and CVE-2015-5114. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5094 | BDU:2015-10721 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3095, CVE-2015-5087, CVE-2015-5100, CVE-2015-5102, CVE-2015-5103, CVE-2015-5104, and CVE-2015-5115. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5093 | BDU:2015-10717 | Buffer overflow in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5092 | Отсутствует | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2014-8450, CVE-2015-4449, CVE-2015-4450, CVE-2015-5088, and CVE-2015-5089. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.0) |
| CVE-2015-5091 | Отсутствует | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to cause a denial of service via invalid data. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7.8) |
| CVE-2015-5090 | Отсутствует | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass intended access restrictions and perform a transition from Low Integrity to Medium Integrity via unspecified vectors, a different vulnerability than CVE-2015-4446 and CVE-2015-5106. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7.2) |
| CVE-2015-5089 | Отсутствует | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2014-8450, CVE-2015-4449, CVE-2015-4450, CVE-2015-5088, and CVE-2015-5092. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.0) |
| CVE-2015-5088 | Отсутствует | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2014-8450, CVE-2015-4449, CVE-2015-4450, CVE-2015-5089, and CVE-2015-5092. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.0) |
| CVE-2015-5087 | BDU:2015-10713 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3095, CVE-2015-5094, CVE-2015-5100, CVE-2015-5102, CVE-2015-5103, CVE-2015-5104, and CVE-2015-5115. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-5086 | BDU:2015-10709 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4435, CVE-2015-4438, CVE-2015-4441, CVE-2015-4445, CVE-2015-4447, CVE-2015-4451, CVE-2015-4452, and CVE-2015-5085. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-5085 | BDU:2015-10705 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4435, CVE-2015-4438, CVE-2015-4441, CVE-2015-4445, CVE-2015-4447, CVE-2015-4451, CVE-2015-4452, and CVE-2015-5086. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-4452 | BDU:2015-10701 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4435, CVE-2015-4438, CVE-2015-4441, CVE-2015-4445, CVE-2015-4447, CVE-2015-4451, CVE-2015-5085, and CVE-2015-5086. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9.3) |
| CVE-2015-4451 | BDU:2015-10697 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4435, CVE-2015-4438, CVE-2015-4441, CVE-2015-4445, CVE-2015-4447, CVE-2015-4452, CVE-2015-5085, and CVE-2015-5086. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9.3) |
| CVE-2015-4450 | Отсутствует | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2014-8450, CVE-2015-4449, CVE-2015-5088, CVE-2015-5089, and CVE-2015-5092. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.0) |
| CVE-2015-4449 | Отсутствует | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2014-8450, CVE-2015-4450, CVE-2015-5088, CVE-2015-5089, and CVE-2015-5092. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.0) |
| CVE-2015-4448 | BDU:2015-10693 | Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5095, CVE-2015-5099, CVE-2015-5101, CVE-2015-5111, CVE-2015-5113, and CVE-2015-5114. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-4447 | BDU:2015-10689 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4435, CVE-2015-4438, CVE-2015-4441, CVE-2015-4445, CVE-2015-4451, CVE-2015-4452, CVE-2015-5085, and CVE-2015-5086. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-4446 | BDU:2015-10874 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass intended access restrictions and perform a transition from Low Integrity to Medium Integrity via unspecified vectors, a different vulnerability than CVE-2015-5090 and CVE-2015-5106. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7.5) |
| CVE-2015-4445 | BDU:2015-10685 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4435, CVE-2015-4438, CVE-2015-4441, CVE-2015-4447, CVE-2015-4451, CVE-2015-4452, CVE-2015-5085, and CVE-2015-5086. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-4444 | Отсутствует | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to cause a denial of service (NULL pointer dereference) via unspecified vectors, a different vulnerability than CVE-2015-4443. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.0) |
| CVE-2015-4443 | Отсутствует | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to cause a denial of service (NULL pointer dereference) via unspecified vectors, a different vulnerability than CVE-2015-4444. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.0) |
| CVE-2015-4441 | BDU:2015-10681 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4435, CVE-2015-4438, CVE-2015-4445, CVE-2015-4447, CVE-2015-4451, CVE-2015-4452, CVE-2015-5085, and CVE-2015-5086. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-4438 | BDU:2015-10677 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4435, CVE-2015-4441, CVE-2015-4445, CVE-2015-4447, CVE-2015-4451, CVE-2015-4452, CVE-2015-5085, and CVE-2015-5086. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-4435 | BDU:2015-10673 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4438, CVE-2015-4441, CVE-2015-4445, CVE-2015-4447, CVE-2015-4451, CVE-2015-4452, CVE-2015-5085, and CVE-2015-5086. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2015-3095 | BDU:2015-10669 | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5087, CVE-2015-5094, CVE-2015-5100, CVE-2015-5102, CVE-2015-5103, CVE-2015-5104, and CVE-2015-5115. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2014-8450 | Отсутствует | Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2015-4449, CVE-2015-4450, CVE-2015-5088, CVE-2015-5089, and CVE-2015-5092. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.0) |

## AIMAT Suite

|  |  |  |  |
| --- | --- | --- | --- |
| Идентификатор CVE | Идентификатор ФСТЭК | Описание уязвимостей | Уровень опасности уязвимости |
| Отсутствует | Отсутствует | Отсутствует | Отсутствует |

## FDSI Configurator-1.6

|  |  |  |  |
| --- | --- | --- | --- |
| Идентификатор CVE | Идентификатор ФСТЭК | Описание уязвимостей | Уровень опасности уязвимости |
| Отсутствует | Отсутствует | Отсутствует | Отсутствует |

## FDSI Modbus 2.5 Driver

|  |  |  |  |
| --- | --- | --- | --- |
| Идентификатор CVE | Идентификатор ФСТЭК | Описание уязвимостей | Уровень опасности уязвимости |
| CVE-2021-36276 | Отсутствует | Dell DBUtilDrv2.sys driver (versions 2.5 and 2.6) contains an insufficient access control vulnerability which may lead to escalation of privileges, denial of service, or information disclosure. Local authenticated user access is required. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.6) |
| CVE-2021-20592 | Отсутствует | Missing synchronization vulnerability in GOT2000 series GT27 model communication driver versions 01.19.000 through 01.39.010, GT25 model communication driver versions 01.19.000 through 01.39.010 and GT23 model communication driver versions 01.19.000 through 01.39.010 and GT SoftGOT2000 versions 1.170C through 1.256S allows a remote unauthenticated attacker to cause DoS condition on the MODBUS/TCP slave communication function of the products by rapidly and repeatedly connecting and disconnecting to and from the MODBUS/TCP communication port on a target. Restart or reset is required to recover. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7.8) |
| CVE-2021-20589 | Отсутствует | Buffer access with incorrect length value vulnerability in GOT2000 series GT27 model communication driver versions 01.19.000 through 01.38.000, GT25 model communication driver versions 01.19.000 through 01.38.000, GT23 model communication driver versions 01.19.000 through 01.38.000 and GT21 model communication driver versions 01.21.000 through 01.39.000, GOT SIMPLE series GS21 model communication driver versions 01.21.000 through 01.39.000, GT SoftGOT2000 versions 1.170C through 1.250L and Tension Controller LE7-40GU-L Screen package data for MODBUS/TCP V1.00 allows a remote unauthenticated attacker to stop the communication function of the products via specially crafted packets. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.0) |
| CVE-2020-7523 | BDU:2020-03998 | Improper Privilege Management vulnerability exists in Schneider Electric Modbus Serial Driver (see security notification for versions) which could cause local privilege escalation when the Modbus Serial Driver service is invoked. The driver does not properly assign, modify, track, or check privileges for an actor, creating an unintended sphere of control for that actor. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.4) |
| CVE-2018-7824 | BDU:2021-04275 | An Externally Controlled Reference to a Resource (CWE-610) vulnerability exists in Schneider Electric Modbus Serial Driver (For 64-bit Windows OS:V3.17 IE 37 and prior , For 32-bit Windows OS:V2.17 IE 27 and prior, and as part of the Driver Suite version:V14.12 and prior) which could allow write access to system files available only to users with SYSTEM privilege or other important user files. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2017-5909 | Отсутствует | The Electronic Funds Source (EFS) Mobile Driver Source app 2.5 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.3) |
| CVE-2015-4142 | BDU:2015-12093 | Integer underflow in the WMM Action frame parser in hostapd 0.5.5 through 2.4 and wpa\_supplicant 0.7.0 through 2.4, when used for AP mode MLME/SME functionality, allows remote attackers to cause a denial of service (crash) via a crafted frame, which triggers an out-of-bounds read. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.3) |
| CVE-2014-0777 | Отсутствует | The Modbus slave/outstation driver in the OPC Drivers 1.0.20 and earlier in IOServer OPC Server allows remote attackers to cause a denial of service (out-of-bounds read and daemon crash) via a crafted packet. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7.8) |
| CVE-2013-0662 | BDU:2017-00202 | Multiple stack-based buffer overflows in ModbusDrv.exe in Schneider Electric Modbus Serial Driver 1.10 through 3.2 allow remote attackers to execute arbitrary code via a large buffer-size value in a Modbus Application Header. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9.3) |
| CVE-2007-2052 | Отсутствует | Off-by-one error in the PyLocale\_strxfrm function in Modules/\_localemodule.c for Python 2.4 and 2.5 causes an incorrect buffer size to be used for the strxfrm function, which allows context-dependent attackers to read portions of memory via unknown manipulations that trigger a buffer over-read due to missing null termination. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.0) |

## FERRET

|  |  |  |  |
| --- | --- | --- | --- |
| Идентификатор CVE | Идентификатор ФСТЭК | Описание уязвимостей | Уровень опасности уязвимости |
| CVE-2015-1374 | Отсутствует | Multiple cross-site request forgery (CSRF) vulnerabilities in admin.php in ferretCMS 1.0.4-alpha allow remote attackers to hijack the authentication of administrators for requests that conduct (1) cross-site scripting (XSS), (2) SQL injection, or (3) unrestricted file upload attacks. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2015-1373 | Отсутствует | Multiple cross-site scripting (XSS) vulnerabilities in admin.php in ferretCMS 1.0.4-alpha allow remote attackers to inject arbitrary web script or HTML via the (1) action parameter in a search request, (2) username in a login request, which is not properly handled when logging the event, or (3) page title in an insert action. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.3) |
| CVE-2015-1372 | Отсутствует | SQL injection vulnerability in ferretCMS 1.0.4-alpha allows remote attackers to execute arbitrary SQL commands via the p parameter in an update action to admin.php. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7.5) |
| CVE-2015-1371 | Отсутствует | Unrestricted file upload vulnerability in ferretCMS 1.0.4-alpha allows remote administrators to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in custom/uploads/. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7.5) |

## FES.WCF

|  |  |  |  |
| --- | --- | --- | --- |
| Идентификатор CVE | Идентификатор ФСТЭК | Описание уязвимостей | Уровень опасности уязвимости |
| Отсутствует | Отсутствует | Отсутствует | Отсутствует |

## Foxboro Classic Software Support

|  |  |  |  |
| --- | --- | --- | --- |
| Идентификатор CVE | Идентификатор ФСТЭК | Описание уязвимостей | Уровень опасности уязвимости |
| Отсутствует | Отсутствует | Отсутствует | Отсутствует |

## Foxboro DCS Control Core Services

|  |  |  |  |
| --- | --- | --- | --- |
| Идентификатор CVE | Идентификатор ФСТЭК | Описание уязвимостей | Уровень опасности уязвимости |
| CVE-2018-7793 | Отсутствует | A Credential Management vulnerability exists in FoxView HMI SCADA (All Foxboro DCS, Foxboro Evo, and IA Series versions prior to Foxboro DCS Control Core Services 9.4 (CCS 9.4) and FoxView 10.5.) which could cause unauthorized disclosure, modification, or disruption in service when the password is modified without permission. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.6) |

## Foxboro DCS System Manager

|  |  |  |  |
| --- | --- | --- | --- |
| Идентификатор CVE | Идентификатор ФСТЭК | Описание уязвимостей | Уровень опасности уязвимости |
| CVE-2022-30313 | BDU:2022-03857 | Honeywell Experion PKS Safety Manager through 2022-05-06 has Missing Authentication for a Critical Function. According to FSCT-2022-0051, there is a Honeywell Experion PKS Safety Manager multiple proprietary protocols with unauthenticated functionality issue. The affected components are characterized as: Honeywell Experion TCP (51000/TCP), Safety Builder (51010/TCP). The potential impact is: Manipulate controller state, Manipulate controller configuration, Manipulate controller logic, Manipulate controller files, Manipulate IO. The Honeywell Experion PKS Distributed Control System (DCS) Safety Manager utilizes several proprietary protocols for a wide variety of functionality, including process data acquisition, controller steering and configuration management. These protocols include: Experion TCP (51000/TCP) and Safety Builder (51010/TCP). None of these protocols have any authentication features, allowing any attacker capable of communicating with the ports in question to invoke (a subset of) desired functionality. There is no authentication functionality on the protocols in question. An attacker capable of invoking the protocols' functionalities could achieve a wide range of adverse impacts, including (but not limited to), the following: for Experion TCP (51000/TCP): Issue IO manipulation commands, Issue file read/write commands; and for Safety Builder (51010/TCP): Issue controller start/stop commands, Issue logic download/upload commands, Issue file read commands, Issue system time change commands. A mitigating factor with regards to some, but not all, of the above functionality is that these require the Safety Manager physical keyswitch to be in the right position. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.6) |
| CVE-2018-7793 | Отсутствует | A Credential Management vulnerability exists in FoxView HMI SCADA (All Foxboro DCS, Foxboro Evo, and IA Series versions prior to Foxboro DCS Control Core Services 9.4 (CCS 9.4) and FoxView 10.5.) which could cause unauthorized disclosure, modification, or disruption in service when the password is modified without permission. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.6) |
| CVE-2014-9206 | Отсутствует | Stack-based buffer overflow in Device Type Manager (DTM) 3.1.6 and earlier for Schneider Electric Invensys SRD Control Valve Positioner devices 960 and 991 allows local users to gain privileges via a malformed DLL file. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.9) |

## Foxboro FVFD 10.6.1 MP76808347

|  |  |  |  |
| --- | --- | --- | --- |
| Идентификатор CVE | Идентификатор ФСТЭК | Описание уязвимостей | Уровень опасности уязвимости |
| CVE-2022-38216 | Отсутствует | An integer overflow exists in Mapbox's closed source gl-native library prior to version 10.6.1, which is bundled with multiple Mapbox products including open source libraries. The overflow is caused by large image height and width values when creating a new Image and allows for out of bounds writes, potentially crashing the Mapbox process. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7.2) |
| CVE-2021-28830 | Отсутствует | The TIBCO Spotfire Server and TIBCO Enterprise Runtime for R components of TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition, TIBCO Enterprise Runtime for R - Server Edition, TIBCO Enterprise Runtime for R - Server Edition, TIBCO Spotfire Analytics Platform for AWS Marketplace, TIBCO Spotfire Server, TIBCO Spotfire Server, TIBCO Spotfire Server, TIBCO Spotfire Statistics Services, TIBCO Spotfire Statistics Services, and TIBCO Spotfire Statistics Services contain a vulnerability that theoretically allows a low privileged attacker with local access on the Windows operating system to insert malicious software. The affected component can be abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from the affected component searching for run-time artifacts outside of the installation hierarchy. Affected releases are TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition: versions 1.2.4 and below, TIBCO Enterprise Runtime for R - Server Edition: versions 1.3.0 and 1.3.1, TIBCO Enterprise Runtime for R - Server Edition: versions 1.4.0, 1.5.0, and 1.6.0, TIBCO Spotfire Analytics Platform for AWS Marketplace: versions 11.3.0 and below, TIBCO Spotfire Server: versions 10.3.12 and below, TIBCO Spotfire Server: versions 10.4.0, 10.5.0, 10.6.0, 10.6.1, 10.7.0, 10.8.0, 10.8.1, 10.9.0, 10.10.0, 10.10.1, 10.10.2, 10.10.3, and 10.10.4, TIBCO Spotfire Server: versions 11.0.0, 11.1.0, 11.2.0, and 11.3.0, TIBCO Spotfire Statistics Services: versions 10.3.0 and below, TIBCO Spotfire Statistics Services: versions 10.10.0, 10.10.1, and 10.10.2, and TIBCO Spotfire Statistics Services: versions 11.1.0, 11.2.0, and 11.3.0. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7.2) |
| CVE-2021-23275 | Отсутствует | The Windows Installation component of TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition, TIBCO Enterprise Runtime for R - Server Edition, TIBCO Enterprise Runtime for R - Server Edition, TIBCO Spotfire Analytics Platform for AWS Marketplace, TIBCO Spotfire Server, TIBCO Spotfire Server, TIBCO Spotfire Server, TIBCO Spotfire Statistics Services, TIBCO Spotfire Statistics Services, and TIBCO Spotfire Statistics Services contains a vulnerability that theoretically allows a low privileged attacker with local access on some versions of the Windows operating system to insert malicious software. The affected component can be abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from a lack of access restrictions on certain files and/or folders in the installation. Affected releases are TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition: versions 1.2.4 and below, TIBCO Enterprise Runtime for R - Server Edition: versions 1.3.0 and 1.3.1, TIBCO Enterprise Runtime for R - Server Edition: versions 1.4.0, 1.5.0, and 1.6.0, TIBCO Spotfire Analytics Platform for AWS Marketplace: versions 11.3.0 and below, TIBCO Spotfire Server: versions 10.3.12 and below, TIBCO Spotfire Server: versions 10.4.0, 10.5.0, 10.6.0, 10.6.1, 10.7.0, 10.8.0, 10.8.1, 10.9.0, 10.10.0, 10.10.1, 10.10.2, 10.10.3, and 10.10.4, TIBCO Spotfire Server: versions 11.0.0, 11.1.0, 11.2.0, and 11.3.0, TIBCO Spotfire Statistics Services: versions 10.3.0 and below, TIBCO Spotfire Statistics Services: versions 10.10.0, 10.10.1, and 10.10.2, and TIBCO Spotfire Statistics Services: versions 11.1.0, 11.2.0, and 11.3.0. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7.2) |
| CVE-2020-9408 | Отсутствует | The Spotfire library component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and TIBCO Spotfire Server contains a vulnerability that theoretically allows an attacker with write permissions to the Spotfire Library, but not "Script Author" group permission, to modify attributes of files and objects saved to the library such that the system treats them as trusted. This could allow an attacker to cause the Spotfire Web Player, Analyst clients, and TERR Service into executing arbitrary code with the privileges of the system account that started those processes. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace: versions 10.8.0 and below and TIBCO Spotfire Server: versions 7.11.9 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.3.0, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, and 10.3.6, versions 10.4.0, 10.5.0, 10.6.0, 10.6.1, 10.7.0, and 10.8.0. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9.0) |
| CVE-2020-7278 | Отсутствует | Exploiting incorrectly configured access control security levels vulnerability in ENS Firewall in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 April 2020 and 10.6.1 April 2020 updates allows remote attackers and local users to allow or block unauthorized traffic via pre-existing rules not being handled correctly when updating to the February 2020 updates. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.0) |
| CVE-2020-7251 | Отсутствует | Improper access control vulnerability in Configuration Tool in McAfee Mcafee Endpoint Security (ENS) Prior to 10.6.1 February 2020 Update allows local users to disable security features via unauthorised use of the configuration tool from older versions of ENS. | Низкий уровень опасности (базовая оценка CVSS 2.0 составляет 2.1) |
| CVE-2020-36652 | BDU:2023-01636 | Incorrect Default Permissions vulnerability in Hitachi Automation Director on Linux, Hitachi Infrastructure Analytics Advisor on Linux (Hitachi Infrastructure Analytics Advisor, Analytics probe server components), Hitachi Ops Center Automator on Linux, Hitachi Ops Center Analyzer on Linux (Hitachi Ops Center Analyzer, Analyzer probe server components), Hitachi Ops Center Viewpoint on Linux (Viewpoint RAID Agent component) allows local users to read and write specific files. This issue affects Hitachi Automation Director: from 8.2.0-00 through 10.6.1-00; Hitachi Infrastructure Analytics Advisor: from 2.0.0-00 through 4.0.0-00; Hitachi Ops Center Automator: before 10.9.1-00; Hitachi Ops Center Analyzer: before 10.9.1-00; Hitachi Ops Center Viewpoint: before 10.9.1-00. | Средний уровень опасности (базовая оценка CVSS 3.0 составляет 6.6) |
| CVE-2019-3653 | Отсутствует | Improper access control vulnerability in Configuration tool in McAfee Endpoint Security (ENS) Prior to 10.6.1 October 2019 Update allows local user to gain access to security configuration via unauthorized use of the configuration tool. | Низкий уровень опасности (базовая оценка CVSS 2.0 составляет 2.1) |
| CVE-2019-3652 | BDU:2020-00026 | Code Injection vulnerability in EPSetup.exe in McAfee Endpoint Security (ENS) Prior to 10.6.1 October 2019 Update allows local user to get their malicious code installed by the ENS installer via code injection into EPSetup.exe by an attacker with access to the installer. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.6) |
| CVE-2019-3586 | Отсутствует | Protection Mechanism Failure in the Firewall in McAfee Endpoint Security (ENS) 10.x prior to 10.6.1 May 2019 update allows context-dependent attackers to circumvent ENS protection where GTI flagged IP addresses are not blocked by the ENS Firewall via specially crafted malicious sites where the GTI reputation is carefully manipulated and does not correctly trigger the ENS Firewall to block the connection. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 5.1) |
| CVE-2019-3582 | Отсутствует | Privilege Escalation vulnerability in Microsoft Windows client in McAfee Endpoint Security (ENS) 10.6.1 and earlier allows local users to gain elevated privileges via a specific set of circumstances. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.1) |
| CVE-2019-16193 | Отсутствует | In ArcGIS Enterprise 10.6.1, a crafted IFRAME element can be used to trigger a Cross Frame Scripting (XFS) attack through the EDIT MY PROFILE feature. | Низкий уровень опасности (базовая оценка CVSS 2.0 составляет 3.5) |
| CVE-2018-7793 | Отсутствует | A Credential Management vulnerability exists in FoxView HMI SCADA (All Foxboro DCS, Foxboro Evo, and IA Series versions prior to Foxboro DCS Control Core Services 9.4 (CCS 9.4) and FoxView 10.5.) which could cause unauthorized disclosure, modification, or disruption in service when the password is modified without permission. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.6) |
| CVE-2018-1080 | Отсутствует | Dogtag PKI, through version 10.6.1, has a vulnerability in AAclAuthz.java that, under certain configurations, causes the application of ACL allow and deny rules to be reversed. If a server is configured to process allow rules before deny rules (authz.evaluateOrder=allow,deny), then allow rules will deny access and deny rules will grant access. This may result in an escalation of privileges or have other unintended consequences. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2017-10857 | Отсутствует | Cybozu Office 10.0.0 to 10.6.1 allows authenticated attackers to bypass access restriction to perform arbitrary actions via "Cabinet" function. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.0) |
| CVE-2016-5312 | Отсутствует | Directory traversal vulnerability in the charting component in Symantec Messaging Gateway before 10.6.2 allows remote authenticated users to read arbitrary files via a .. (dot dot) in the sn parameter to brightmail/servlet/com.ve.kavachart.servlet.ChartStream. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.0) |
| CVE-2016-3646 | BDU:2016-01695 | The AntiVirus Decomposer engine in Symantec Advanced Threat Protection (ATP); Symantec Data Center Security:Server (SDCS:S) 6.x through 6.6 MP1; Symantec Web Gateway; Symantec Endpoint Protection (SEP) before 12.1 RU6 MP5; Symantec Endpoint Protection (SEP) for Mac; Symantec Endpoint Protection (SEP) for Linux before 12.1 RU6 MP5; Symantec Protection Engine (SPE) before 7.0.5 HF01, 7.5.x before 7.5.3 HF03, 7.5.4 before HF01, and 7.8.0 before HF01; Symantec Protection for SharePoint Servers (SPSS) 6.0.3 through 6.0.5 before 6.0.5 HF 1.5 and 6.0.6 before HF 1.6; Symantec Mail Security for Microsoft Exchange (SMSMSE) before 7.0\_3966002 HF1.1 and 7.5.x before 7.5\_3966008 VHF1.2; Symantec Mail Security for Domino (SMSDOM) before 8.0.9 HF1.1 and 8.1.x before 8.1.3 HF1.2; CSAPI before 10.0.4 HF01; Symantec Message Gateway (SMG) before 10.6.1-4; Symantec Message Gateway for Service Providers (SMG-SP) 10.5 before patch 254 and 10.6 before patch 253; Norton AntiVirus, Norton Security, Norton Internet Security, and Norton 360 before NGC 22.7; Norton Security for Mac before 13.0.2; Norton Power Eraser (NPE) before 5.1; and Norton Bootable Removal Tool (NBRT) before 2016.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory access violation) via a crafted ZIP archive that is mishandled during decompression. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-3645 | BDU:2016-01696 | Integer overflow in the TNEF unpacker in the AntiVirus Decomposer engine in Symantec Advanced Threat Protection (ATP); Symantec Data Center Security:Server (SDCS:S) 6.x through 6.6 MP1; Symantec Web Gateway; Symantec Endpoint Protection (SEP) before 12.1 RU6 MP5; Symantec Endpoint Protection (SEP) for Mac; Symantec Endpoint Protection (SEP) for Linux before 12.1 RU6 MP5; Symantec Protection Engine (SPE) before 7.0.5 HF01, 7.5.x before 7.5.3 HF03, 7.5.4 before HF01, and 7.8.0 before HF01; Symantec Protection for SharePoint Servers (SPSS) 6.0.3 through 6.0.5 before 6.0.5 HF 1.5 and 6.0.6 before HF 1.6; Symantec Mail Security for Microsoft Exchange (SMSMSE) before 7.0\_3966002 HF1.1 and 7.5.x before 7.5\_3966008 VHF1.2; Symantec Mail Security for Domino (SMSDOM) before 8.0.9 HF1.1 and 8.1.x before 8.1.3 HF1.2; CSAPI before 10.0.4 HF01; Symantec Message Gateway (SMG) before 10.6.1-4; Symantec Message Gateway for Service Providers (SMG-SP) 10.5 before patch 254 and 10.6 before patch 253; Norton AntiVirus, Norton Security, Norton Internet Security, and Norton 360 before NGC 22.7; Norton Security for Mac before 13.0.2; Norton Power Eraser (NPE) before 5.1; and Norton Bootable Removal Tool (NBRT) before 2016.1 allows remote attackers to have an unspecified impact via crafted TNEF data. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-3644 | BDU:2016-01697 | The AntiVirus Decomposer engine in Symantec Advanced Threat Protection (ATP); Symantec Data Center Security:Server (SDCS:S) 6.x through 6.6 MP1; Symantec Web Gateway; Symantec Endpoint Protection (SEP) before 12.1 RU6 MP5; Symantec Endpoint Protection (SEP) for Mac; Symantec Endpoint Protection (SEP) for Linux before 12.1 RU6 MP5; Symantec Protection Engine (SPE) before 7.0.5 HF01, 7.5.x before 7.5.3 HF03, 7.5.4 before HF01, and 7.8.0 before HF01; Symantec Protection for SharePoint Servers (SPSS) 6.0.3 through 6.0.5 before 6.0.5 HF 1.5 and 6.0.6 before HF 1.6; Symantec Mail Security for Microsoft Exchange (SMSMSE) before 7.0\_3966002 HF1.1 and 7.5.x before 7.5\_3966008 VHF1.2; Symantec Mail Security for Domino (SMSDOM) before 8.0.9 HF1.1 and 8.1.x before 8.1.3 HF1.2; CSAPI before 10.0.4 HF01; Symantec Message Gateway (SMG) before 10.6.1-4; Symantec Message Gateway for Service Providers (SMG-SP) 10.5 before patch 254 and 10.6 before patch 253; Norton AntiVirus, Norton Security, Norton Internet Security, and Norton 360 before NGC 22.7; Norton Security for Mac before 13.0.2; Norton Power Eraser (NPE) before 5.1; and Norton Bootable Removal Tool (NBRT) before 2016.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via modified MIME data in a message. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-2211 | BDU:2016-01701 | The AntiVirus Decomposer engine in Symantec Advanced Threat Protection (ATP); Symantec Data Center Security:Server (SDCS:S) 6.x through 6.6 MP1; Symantec Web Gateway; Symantec Endpoint Protection (SEP) before 12.1 RU6 MP5; Symantec Endpoint Protection (SEP) for Mac; Symantec Endpoint Protection (SEP) for Linux before 12.1 RU6 MP5; Symantec Protection Engine (SPE) before 7.0.5 HF01, 7.5.x before 7.5.3 HF03, 7.5.4 before HF01, and 7.8.0 before HF01; Symantec Protection for SharePoint Servers (SPSS) 6.0.3 through 6.0.5 before 6.0.5 HF 1.5 and 6.0.6 before HF 1.6; Symantec Mail Security for Microsoft Exchange (SMSMSE) before 7.0\_3966002 HF1.1 and 7.5.x before 7.5\_3966008 VHF1.2; Symantec Mail Security for Domino (SMSDOM) before 8.0.9 HF1.1 and 8.1.x before 8.1.3 HF1.2; CSAPI before 10.0.4 HF01; Symantec Message Gateway (SMG) before 10.6.1-4; Symantec Message Gateway for Service Providers (SMG-SP) 10.5 before patch 254 and 10.6 before patch 253; Norton AntiVirus, Norton Security, Norton Internet Security, and Norton 360 before NGC 22.7; Norton Security for Mac before 13.0.2; Norton Power Eraser (NPE) before 5.1; and Norton Bootable Removal Tool (NBRT) before 2016.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted CAB file that is mishandled during decompression. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9.3) |
| CVE-2016-2210 | BDU:2016-01702 | Buffer overflow in Dec2LHA.dll in the AntiVirus Decomposer engine in Symantec Advanced Threat Protection (ATP); Symantec Data Center Security:Server (SDCS:S) 6.x through 6.6 MP1; Symantec Web Gateway; Symantec Endpoint Protection (SEP) before 12.1 RU6 MP5; Symantec Endpoint Protection (SEP) for Mac; Symantec Endpoint Protection (SEP) for Linux before 12.1 RU6 MP5; Symantec Protection Engine (SPE) before 7.0.5 HF01, 7.5.x before 7.5.3 HF03, 7.5.4 before HF01, and 7.8.0 before HF01; Symantec Protection for SharePoint Servers (SPSS) 6.0.3 through 6.0.5 before 6.0.5 HF 1.5 and 6.0.6 before HF 1.6; Symantec Mail Security for Microsoft Exchange (SMSMSE) before 7.0\_3966002 HF1.1 and 7.5.x before 7.5\_3966008 VHF1.2; Symantec Mail Security for Domino (SMSDOM) before 8.0.9 HF1.1 and 8.1.x before 8.1.3 HF1.2; CSAPI before 10.0.4 HF01; Symantec Message Gateway (SMG) before 10.6.1-4; Symantec Message Gateway for Service Providers (SMG-SP) 10.5 before patch 254 and 10.6 before patch 253; Norton AntiVirus, Norton Security, Norton Internet Security, and Norton 360 before NGC 22.7; Norton Security for Mac before 13.0.2; Norton Power Eraser (NPE) before 5.1; and Norton Bootable Removal Tool (NBRT) before 2016.1 allows remote attackers to execute arbitrary code via a crafted file. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9.0) |
| CVE-2016-2209 | BDU:2016-01703 | Buffer overflow in Dec2SS.dll in the AntiVirus Decomposer engine in Symantec Advanced Threat Protection (ATP); Symantec Data Center Security:Server (SDCS:S) 6.x through 6.6 MP1; Symantec Web Gateway; Symantec Endpoint Protection (SEP) before 12.1 RU6 MP5; Symantec Endpoint Protection (SEP) for Mac; Symantec Endpoint Protection (SEP) for Linux before 12.1 RU6 MP5; Symantec Protection Engine (SPE) before 7.0.5 HF01, 7.5.x before 7.5.3 HF03, 7.5.4 before HF01, and 7.8.0 before HF01; Symantec Protection for SharePoint Servers (SPSS) 6.0.3 through 6.0.5 before 6.0.5 HF 1.5 and 6.0.6 before HF 1.6; Symantec Mail Security for Microsoft Exchange (SMSMSE) before 7.0\_3966002 HF1.1 and 7.5.x before 7.5\_3966008 VHF1.2; Symantec Mail Security for Domino (SMSDOM) before 8.0.9 HF1.1 and 8.1.x before 8.1.3 HF1.2; CSAPI before 10.0.4 HF01; Symantec Message Gateway (SMG) before 10.6.1-4; Symantec Message Gateway for Service Providers (SMG-SP) 10.5 before patch 254 and 10.6 before patch 253; Norton AntiVirus, Norton Security, Norton Internet Security, and Norton 360 before NGC 22.7; Norton Security for Mac before 13.0.2; Norton Power Eraser (NPE) before 5.1; and Norton Bootable Removal Tool (NBRT) before 2016.1 allows remote attackers to execute arbitrary code via a crafted file. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9.0) |
| CVE-2016-2207 | BDU:2016-01704 | The AntiVirus Decomposer engine in Symantec Advanced Threat Protection (ATP); Symantec Data Center Security:Server (SDCS:S) 6.x through 6.6 MP1; Symantec Web Gateway; Symantec Endpoint Protection (SEP) before 12.1 RU6 MP5; Symantec Endpoint Protection (SEP) for Mac; Symantec Endpoint Protection (SEP) for Linux before 12.1 RU6 MP5; Symantec Protection Engine (SPE) before 7.0.5 HF01, 7.5.x before 7.5.3 HF03, 7.5.4 before HF01, and 7.8.0 before HF01; Symantec Protection for SharePoint Servers (SPSS) 6.0.3 through 6.0.5 before 6.0.5 HF 1.5 and 6.0.6 before HF 1.6; Symantec Mail Security for Microsoft Exchange (SMSMSE) before 7.0\_3966002 HF1.1 and 7.5.x before 7.5\_3966008 VHF1.2; Symantec Mail Security for Domino (SMSDOM) before 8.0.9 HF1.1 and 8.1.x before 8.1.3 HF1.2; CSAPI before 10.0.4 HF01; Symantec Message Gateway (SMG) before 10.6.1-4; Symantec Message Gateway for Service Providers (SMG-SP) 10.5 before patch 254 and 10.6 before patch 253; Norton AntiVirus, Norton Security, Norton Internet Security, and Norton 360 before NGC 22.7; Norton Security for Mac before 13.0.2; Norton Power Eraser (NPE) before 5.1; and Norton Bootable Removal Tool (NBRT) before 2016.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory access violation) via a crafted RAR file that is mishandled during decompression. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2016-2204 | Отсутствует | The management console on Symantec Messaging Gateway (SMG) Appliance devices before 10.6.1 allows local users to obtain root-shell access via crafted terminal-window input. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.5) |
| CVE-2016-2203 | Отсутствует | The management console on Symantec Messaging Gateway (SMG) Appliance devices before 10.6.1 allows local users to discover an encrypted AD password by leveraging certain read privileges. | Низкий уровень опасности (базовая оценка CVSS 2.0 составляет 2.1) |
| CVE-2014-9206 | Отсутствует | Stack-based buffer overflow in Device Type Manager (DTM) 3.1.6 and earlier for Schneider Electric Invensys SRD Control Valve Positioner devices 960 and 991 allows local users to gain privileges via a malformed DLL file. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.9) |
| CVE-2014-5503 | Отсутствует | SQL injection vulnerability in the Guest Login Portal in the Sophos Cyberoam appliances with CyberoamOS before 10.6.1 GA allows remote attackers to execute arbitrary SQL commands via the add\_guest\_user opcode. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2014-5502 | Отсутствует | The Sophos Cyberoam appliances with CyberoamOS before 10.6.1 GA allows remote authenticated users to inject arbitrary commands via a (1) checkcert\_key, (2) webclient\_portal\_settings, (3) sslvpn\_liveuser\_delete, or (4) ccc\_flush\_sql\_file opcode. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9.0) |
| CVE-2014-5501 | Отсутствует | Stack-based buffer overflow in the diagnose service in the Sophos Cyberoam appliances with CyberoamOS before 10.6.1 GA allows remote attackers to execute arbitrary code via a crafted webpage or file. | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9.3) |
| CVE-2012-3005 | Отсутствует | Untrusted search path vulnerability in Invensys Wonderware InTouch 2012 and earlier, as used in Wonderware Application Server, Wonderware Information Server, Foxboro Control Software, InFusion CE/FE/SCADA, InBatch, and Wonderware Historian, allows local users to gain privileges via a Trojan horse DLL in an unspecified directory. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.9) |
| CVE-2012-0258 | Отсутствует | Heap-based buffer overflow in the WWCabFile ActiveX component in the Wonderware System Platform in Invensys Wonderware Application Server 2012 and earlier, Foxboro Control Software 3.1 and earlier, InFusion CE/FE/SCADA 2.5 and earlier, Wonderware Information Server 4.5 and earlier, ArchestrA Application Object Toolkit 3.2 and earlier, and InTouch 10.0 through 10.5 might allow remote attackers to execute arbitrary code via a long string to the AddFile member. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2012-0257 | Отсутствует | Heap-based buffer overflow in the WWCabFile ActiveX component in the Wonderware System Platform in Invensys Wonderware Application Server 2012 and earlier, Foxboro Control Software 3.1 and earlier, InFusion CE/FE/SCADA 2.5 and earlier, Wonderware Information Server 4.5 and earlier, ArchestrA Application Object Toolkit 3.2 and earlier, and InTouch 10.0 through 10.5 might allow remote attackers to execute arbitrary code via a long string to the Open member, leading to a function-pointer overwrite. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2011-4870 | Отсутствует | Multiple buffer overflows in the (1) GUIControls, (2) BatchObjSrv, and (3) BatchSecCtrl ActiveX controls in Invensys Wonderware InBatch 9.0 and 9.0 SP1, and InBatch 8.1 SP1, 9.0 SP2, and 9.5 Server and Runtime Clients, allow remote attackers to execute arbitrary code via a long string in a property value, a different issue than CVE-2011-3141. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2010-4557 | Отсутствует | Buffer overflow in the lm\_tcp service in Invensys Wonderware InBatch 8.1 and 9.0, as used in Invensys Foxboro I/A Series Batch 8.1 and possibly other products, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted request to port 9001. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |
| CVE-2008-1704 | Отсутствует | Multiple buffer overflows in TIBCO Software Enterprise Message Service (EMS) before 4.4.3, and iProcess Engine 10.6.0 through 10.6.1, allow remote attackers to execute arbitrary code via a crafted message to the EMS server. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |

## Foxboro GD50419045

|  |  |  |  |
| --- | --- | --- | --- |
| Идентификатор CVE | Идентификатор ФСТЭК | Описание уязвимостей | Уровень опасности уязвимости |
| CVE-2018-7793 | Отсутствует | A Credential Management vulnerability exists in FoxView HMI SCADA (All Foxboro DCS, Foxboro Evo, and IA Series versions prior to Foxboro DCS Control Core Services 9.4 (CCS 9.4) and FoxView 10.5.) which could cause unauthorized disclosure, modification, or disruption in service when the password is modified without permission. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.6) |
| CVE-2014-9206 | Отсутствует | Stack-based buffer overflow in Device Type Manager (DTM) 3.1.6 and earlier for Schneider Electric Invensys SRD Control Valve Positioner devices 960 and 991 allows local users to gain privileges via a malformed DLL file. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.9) |
| CVE-2012-3005 | Отсутствует | Untrusted search path vulnerability in Invensys Wonderware InTouch 2012 and earlier, as used in Wonderware Application Server, Wonderware Information Server, Foxboro Control Software, InFusion CE/FE/SCADA, InBatch, and Wonderware Historian, allows local users to gain privileges via a Trojan horse DLL in an unspecified directory. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.9) |
| CVE-2012-0258 | Отсутствует | Heap-based buffer overflow in the WWCabFile ActiveX component in the Wonderware System Platform in Invensys Wonderware Application Server 2012 and earlier, Foxboro Control Software 3.1 and earlier, InFusion CE/FE/SCADA 2.5 and earlier, Wonderware Information Server 4.5 and earlier, ArchestrA Application Object Toolkit 3.2 and earlier, and InTouch 10.0 through 10.5 might allow remote attackers to execute arbitrary code via a long string to the AddFile member. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2012-0257 | Отсутствует | Heap-based buffer overflow in the WWCabFile ActiveX component in the Wonderware System Platform in Invensys Wonderware Application Server 2012 and earlier, Foxboro Control Software 3.1 and earlier, InFusion CE/FE/SCADA 2.5 and earlier, Wonderware Information Server 4.5 and earlier, ArchestrA Application Object Toolkit 3.2 and earlier, and InTouch 10.0 through 10.5 might allow remote attackers to execute arbitrary code via a long string to the Open member, leading to a function-pointer overwrite. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2011-4870 | Отсутствует | Multiple buffer overflows in the (1) GUIControls, (2) BatchObjSrv, and (3) BatchSecCtrl ActiveX controls in Invensys Wonderware InBatch 9.0 and 9.0 SP1, and InBatch 8.1 SP1, 9.0 SP2, and 9.5 Server and Runtime Clients, allow remote attackers to execute arbitrary code via a long string in a property value, a different issue than CVE-2011-3141. | Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6.8) |
| CVE-2010-4557 | Отсутствует | Buffer overflow in the lm\_tcp service in Invensys Wonderware InBatch 8.1 and 9.0, as used in Invensys Foxboro I/A Series Batch 8.1 and possibly other products, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted request to port 9001. | Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10.0) |