You are here:

Pexip security bulletins

The following security bulletins are published by Pexip for issues affecting our own products — Pexip Infinity, the Pexip apps, the VMR self-service portal, Enhanced Room Management and the AI Media Server (AIMS). There are no recent security bulletins for any other Pexip products, including the Reverse Proxy and TURN Server. See the respective release notes for Pexip Secure Meetings for Justice and Pexip Secure Scheduler for Web.

For information about external issues arising in third-party software and operating systems that may impact these Pexip products, see https://www.pexip.com/trust-center. Where relevant, updates will be incorporated into each Pexip product, so we recommend that you frequently check for and always run the latest versions of each product. If you have deployed Pexip's VMR self-service portal, Reverse Proxy and TURN Server or Pexip Justice products, you should also ensure that the appliance's operating system is regularly patched against the latest security bugs.

More information specific for each of the vulnerabilities can be found via the NIST National Vulnerability Database: http://nvd.nist.gov/.

> Where a CVE ID is pending allocation, a placeholder reference beginning “PEXTEMP-” is used. These references will be updated when official CVE IDs are available.

Pexip Infinity

This list covers issues addressed in Pexip Infinity v38.0 and later. For issues addressed in v37.x or earlier, see our documentation for previous releases.

Each bulletin addresses a number of vulnerabilities in the operating system software used by Pexip Infinity. The bulletins include an assessment of the issues, the impact to the Pexip Infinity platform, and resolution details.

In the table below, "Severity" reflects the severity of the issue as calculated from the CVSS Base Score. "Risk" reflects the risk associated with each vulnerability in the context of the Pexip Infinity product environment.

Reference	Description	Severity	Risk	Updated	Impacted versions	Addressed in version
CVE-2026-103099	Insufficient input validation in the media implementation allows a remote attacker to trigger a software abort resulting in a denial of service. **CVSS 3.1 base score**: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Discussion**: A crafted media stream may result in a controlled abort during processing. **Mitigation**: None. **Resolution**: Upgrade to Pexip Infinity v41.1 or later.	High	High	August 2026	18 through 41	41.1
Multiple	**Resolved minor issues:** CVE-2025-10148, CVE-2025-13034, CVE-2025-14524, CVE-2025-14819, CVE-2025-49794, CVE-2025-59375, CVE-2025-8732, CVE-2026-0989, CVE-2026-0990, CVE-2026-0992, CVE-2026-10723, CVE-2026-10822, CVE-2026-1502, CVE-2026-1757, CVE-2026-1965, CVE-2026-2243, CVE-2026-24515, CVE-2026-25210, CVE-2026-3196, CVE-2026-3276, CVE-2026-32776, CVE-2026-32777, CVE-2026-32778, CVE-2026-34743, CVE-2026-3783, CVE-2026-3784, CVE-2026-3805, CVE-2026-39373, CVE-2026-41080, CVE-2026-42055, CVE-2026-42308, CVE-2026-42310, CVE-2026-42311, CVE-2026-44431, CVE-2026-45186, CVE-2026-45232, CVE-2026-45409, CVE-2026-48142, CVE-2026-4873, CVE-2026-48914, CVE-2026-50219, CVE-2026-50593, CVE-2026-5545, CVE-2026-56131, CVE-2026-56132, CVE-2026-56403, CVE-2026-56404, CVE-2026-56405, CVE-2026-56406, CVE-2026-56407, CVE-2026-56408, CVE-2026-56409, CVE-2026-56410, CVE-2026-56411, CVE-2026-56412, CVE-2026-5773, CVE-2026-6019, CVE-2026-6253, CVE-2026-6276, CVE-2026-6429, CVE-2026-7168, CVE-2026-7774, CVE-2026-8328, CVE-2026-9669			August 2026		41.1
CVE-2026-103110	Improper input validation allows a remote attacker to execute code remotely as an unprivileged user on a Pexip Infinity Conferencing Node. **CVSS3.1 base score:** 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) **Mitigation:** Please contact your Pexip authorized support representative for discussion of mitigation options if an upgrade is not immediately possible. **Resolution:** Upgrade to Pexip Infinity v41, v40.1, v39.2, or v38.2 **Credit:** This issue was responsibly disclosed by Oddmund Skogen.	Critical	Critical	July 2026	All before 38.2, plus 39.0, 39.1 and 40.0	38.2, 39.2, 40.1, 41.0
CVE-2026-103109	Insufficient input validation in the media implementation allows a remote attacker to trigger memory corruption or a software abort resulting in a denial of service. **CVSS3.1 base score:** 7.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H) **Discussion:** A crafted media stream may result in a controlled abort during processing, and has the potential to achieve memory corruption. **Mitigation:** Please contact your Pexip authorized support representative for discussion of mitigation options if an upgrade is not immediately possible. **Resolution:** Upgrade to Pexip Infinity v41, v40.1, v39.2, or v38.2 **Credit:** This issue was responsibly disclosed by Oddmund Skogen.	High	High	July 2026	All before 38.2, plus 39.0, 39.1 and 40.0	38.2, 39.2, 40.1, 41.0

Reference	Description	Severity	Risk	Updated	Impacted versions	Addressed in version
CVE-2026-103108	Insufficient input validation in the media implementation allows a remote attacker to trigger a software abort resulting in a denial of service **CVSS3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Discussion:** A crafted media stream may result in a controlled abort during processing. **Mitigation:** Please contact your Pexip authorized support representative for discussion of mitigation options if an upgrade is not immediately possible. **Resolution:** Upgrade to Pexip Infinity v41, v40.1, v39.2, or v38.2 **Credit:** This issue was responsibly disclosed by Oddmund Skogen.	High	High	July 2026	All before 38.2, plus 39.0, 39.1 and 40.0	38.2, 39.2, 40.1, 41.0
CVE-2026-103106	Improper input validation within an internal Pexip Infinity service allows an attacker with local access to escalate privileges to root. **CVSS3.1 base score:** 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) **Discussion:** Exploitation requires an attacker to be able to run arbitrary code on a node by either achieving remote code execution via some other vulnerability or having administrative access to the operating system. **Mitigation:** None **Resolution:** Upgrade to Pexip Infinity v41, v40.1, v39.2, or v38.2 **Credit:** This issue was responsibly disclosed by Oddmund Skogen.	High	High	July 2026	All before 38.2, plus 39.0, 39.1 and 40.0	38.2, 39.2, 40.1, 41.0
CVE-2026-103105	Improper access control on a product-internal API allows an attacker with local access to a node within a Pexip Infinity installation to execute arbitrary code as an unprivileged user on another Pexip Infinity node. **CVSS3.1 base score:** 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H **Discussion:** Exploitation requires an attacker to be able to run arbitrary code on a node by either achieving remote code execution via some other vulnerability or having administrative access to the operating system. **Mitigation:** None **Resolution:** Upgrade to Pexip Infinity v41, v40.1, v39.2, or v38.2 **Credit:** This issue was responsibly disclosed by Oddmund Skogen.	High	High	July 2026	All before 38.2, plus 39.0, 39.1 and 40.0	38.2, 39.2, 40.1, 41.0
CVE-2026-103100	Insufficient input validation in the signalling implementation allows a malicious attacker to trigger a software abort resulting in a denial of service. **CVSS3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Mitigation:** None **Resolution:** Upgrade to Pexip Infinity v40.1 or v41.0	High	High	July 2026	All before 40.1	40.1 and 41.0
CVE-2026-103104	Insufficient input validation in the media implementation allows a remote attacker to trigger a software abort resulting in a denial of service. **CVSS3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Discussion:** Exploitation of this issue requires an attacker having joined a VMR using a WebRTC/API client. **Mitigation:** None **Resolution:** Upgrade to Pexip Infinity v41.0	High	High	July 2026	35.0 to 40.1	41.0
CVE-2026-103102	Insufficient input validation in the signalling implementation allows a remote attacker to trigger a software abort resulting in a denial of service. **CVSS3.1 base score:** 8.6 (AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H) **Discussion:** Exploitation of this issue requires accessing a gateway call from a WebRTC/API client. **Mitigation:** None **Resolution:** Upgrade to Pexip Infinity v41.0	High	High	July 2026	All before 41.0	41.0

Reference	Description	Severity	Risk	Updated	Impacted versions	Addressed in version
CVE-2026-103101	Insufficient input validation in the web server allows a malicious attacker to render a Pexip Infinity node inaccessible. **CVSS3.1 base score:** 8.6 (AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H) **Mitigation:** None **Resolution:** Upgrade to Pexip Infinity v41.0	High	High	July 2026	30 to 40.1	41.0
CVE-2026-50598	Insufficient input validation in the media implementation allows a remote attacker to trigger a software abort resulting in a denial of service. **CVSS3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Mitigation:** None **Resolution:** Upgrade to Pexip Infinity v41.0	High	High	July 2026	All before 41.0	41.0
CVE-2026-50599	Insufficient input validation in the media implementation allows a remote attacker to trigger a software abort resulting in a denial of service. **CVSS3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Mitigation:** None **Resolution:** Upgrade to Pexip Infinity v41.0	High	High	July 2026	All before 41.0	41.0
CVE-2026-50600	Insufficient input validation in the media implementation allows a remote attacker to trigger a software abort resulting in a denial of service. **CVSS3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Mitigation:** None **Resolution:** Upgrade to Pexip Infinity v41.0	High	High	July 2026	All before 41.0	41.0
CVE-2026-30922	pyasn1 is a generic ASN.1 library for Python. Prior to 0.6.3, the `pyasn1` library is vulnerable to a Denial of Service (DoS) attack caused by uncontrolled recursion when decoding ASN.1 data with deeply nested structures. **CVSS 3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Discussion:** Exploitation on a Pexip Infinity Management Node would require the presentation of a malicious TLS certificate, either by a malicious intermediary or a client if HTTP client certificate authentication, and could cause a denial of service. Exploitation on a Conferencing Node would require a malicious intermediary in order to cause a denial of service. **Mitigation:** Access to the Management Node should be restricted to trusted networks. Administrators should ensure that only trusted HTTP proxies are configured. **Resolution:** Upgrade to Pexip Infinity v41.0	High	High	July 2026	All before 41.0	41.0

Reference	Description	Severity	Risk	Updated	Impacted versions	Addressed in version
Multiple	**Resolved minor issues:** CVE-2016-1000107, CVE-2022-48303, CVE-2023-1264, CVE-2023-1355, CVE-2023-25193, CVE-2023-2609, CVE-2023-2610, CVE-2023-28746, CVE-2023-28858, CVE-2023-29483, CVE-2023-29491, CVE-2023-2953, CVE-2023-30608, CVE-2023-30630, CVE-2023-32681, CVE-2023-33204, CVE-2023-36054, CVE-2023-3896, CVE-2023-39804, CVE-2023-42363, CVE-2023-4255, CVE-2023-45853, CVE-2023-46246, CVE-2023-4692, CVE-2023-4693, CVE-2023-4733, CVE-2023-4734, CVE-2023-4735, CVE-2023-4738, CVE-2023-4750, CVE-2023-4752, CVE-2023-4781, CVE-2023-48231, CVE-2023-48232, CVE-2023-48233, CVE-2023-48234, CVE-2023-48235, CVE-2023-48236, CVE-2023-48237, CVE-2023-48706, CVE-2023-50447, CVE-2023-50782, CVE-2023-5344, CVE-2023-5441, CVE-2023-5535, CVE-2023-7042, CVE-2024-1135, CVE-2024-21823, CVE-2024-22099, CVE-2024-2312, CVE-2024-23829, CVE-2024-25110, CVE-2024-26130, CVE-2024-26462, CVE-2024-26653, CVE-2024-26654, CVE-2024-26655, CVE-2024-26656, CVE-2024-26657, CVE-2024-26756, CVE-2024-26757, CVE-2024-26758, CVE-2024-27010, CVE-2024-27012, CVE-2024-27079, CVE-2024-27099, CVE-2024-27306, CVE-2024-27398, CVE-2024-27399, CVE-2024-27401, CVE-2024-29195, CVE-2024-35195, CVE-2024-35808, CVE-2024-35843, CVE-2024-35949, CVE-2024-36013, CVE-2024-36014, CVE-2024-38608, CVE-2024-39486, CVE-2024-40999, CVE-2024-41010, CVE-2024-41016, CVE-2024-41023, CVE-2024-41045, CVE-2024-41082, CVE-2024-41085, CVE-2024-41957, CVE-2024-41965, CVE-2024-42162, CVE-2024-42317, CVE-2024-43374, CVE-2024-4340, CVE-2024-43790, CVE-2024-43802, CVE-2024-44945, CVE-2024-45306, CVE-2024-46681, CVE-2024-46698, CVE-2024-46701, CVE-2024-46754, CVE-2024-46834, CVE-2024-46869, CVE-2024-47081, CVE-2024-47702, CVE-2024-47703, CVE-2024-47794, CVE-2024-47814, CVE-2024-49885, CVE-2024-49888, CVE-2024-49940, CVE-2024-49968, CVE-2024-50028, CVE-2024-50066, CVE-2024-50102, CVE-2024-5187, CVE-2024-53114, CVE-2024-53147, CVE-2024-53219, CVE-2024-56647, CVE-2024-56702, CVE-2024-56732, CVE-2024-57804, CVE-2024-57974, CVE-2024-57982, CVE-2024-57994, CVE-2024-58093, CVE-2024-8805, CVE-2025-13473, CVE-2025-14550, CVE-2025-14876, CVE-2025-15281, CVE-2025-15467, CVE-2025-21634, CVE-2025-21635, CVE-2025-21682, CVE-2025-21696, CVE-2025-21714, CVE-2025-21723, CVE-2025-21732, CVE-2025-21768, CVE-2025-21825, CVE-2025-21861, CVE-2025-21868, CVE-2025-21884, CVE-2025-21888, CVE-2025-21892, CVE-2025-21907, CVE-2025-21927, CVE-2025-21961, CVE-2025-21976, CVE-2025-22103, CVE-2025-22105, CVE-2025-22106, CVE-2025-22108, CVE-2025-22109, CVE-2025-22111, CVE-2025-22113, CVE-2025-22121, CVE-2025-22125, CVE-2025-23143, CVE-2025-31498, CVE-2025-37759, CVE-2025-37807, CVE-2025-37834, CVE-2025-37861, CVE-2025-37920, CVE-2025-37945, CVE-2025-38022, CVE-2025-38038, CVE-2025-38057, CVE-2025-38064, CVE-2025-38129, CVE-2025-38140, CVE-2025-38162, CVE-2025-38201, CVE-2025-38206, CVE-2025-38234, CVE-2025-38248, CVE-2025-38264, CVE-2025-38279, CVE-2025-38351, CVE-2025-38491, CVE-2025-38499, CVE-2025-38500, CVE-2025-38502, CVE-2025-38528, CVE-2025-38537, CVE-2025-38539, CVE-2025-38540, CVE-2025-38550, CVE-2025-38552, CVE-2025-38556, CVE-2025-38560, CVE-2025-38563, CVE-2025-38565, CVE-2025-38568, CVE-2025-38572, CVE-2025-38584, CVE-2025-38591, CVE-2025-38608, CVE-2025-38614, CVE-2025-38616, CVE-2025-38617, CVE-2025-38618, CVE-2025-38622, CVE-2025-38639, CVE-2025-38640, CVE-2025-38645, CVE-2025-38653, CVE-2025-38678, CVE-2025-38681, CVE-2025-38684, CVE-2025-38685, CVE-2025-38692, CVE-2025-38700, CVE-2025-38701, CVE-2025-38702, CVE-2025-38704, CVE-2025-38708, CVE-2025-38709, CVE-2025-38717, CVE-2025-38721, CVE-2025-38730, CVE-2025-38732, CVE-2025-38734, CVE-2025-38735, CVE-2025-39677, CVE-2025-39681, CVE-2025-39682, CVE-2025-39683, CVE-2025-39689, CVE-2025-39691, CVE-2025-39702, CVE-2025-39718, CVE-2025-39724, CVE-2025-39726, CVE-2025-39744, CVE-2025-39748, CVE-2025-39749, CVE-2025-39754, CVE-2025-39756, CVE-2025-39763, CVE-2025-39764, CVE-2025-39766, CVE-2025-39773, CVE-2025-39782, CVE-2025-39789, CVE-2025-39790, CVE-2025-39795, CVE-2025-39797, CVE-2025-39810, CVE-2025-39813, CVE-2025-39817, CVE-2025-39823, CVE-2025-39826, CVE-2025-39829, CVE-2025-39832, CVE-2025-39843, CVE-2025-39844, CVE-2025-39845, CVE-2025-39850, CVE-2025-39851, CVE-2025-39857, CVE-2025-39866, CVE-2025-39880, CVE-2025-39881, CVE-2025-39883, CVE-2025-39886, CVE-2025-39895, CVE-2025-39902, CVE-2025-39910, CVE-2025-39913, CVE-2025-39914, CVE-2025-39931, CVE-2025-39940, CVE-2025-39946, CVE-2025-39947, CVE-2025-39953, CVE-2025-39955, CVE-2025-39964, CVE-2025-39967, CVE-2025-39977, CVE-2025-39980, CVE-2025-39990, CVE-2025-39998, CVE-2025-40001, CVE-2025-40003, CVE-2025-40006, CVE-2025-40018, CVE-2025-40019, CVE-2025-40021, CVE-2025-40024, CVE-2025-40026, CVE-2025-40038, CVE-2025-40040, CVE-2025-40042, CVE-2025-40044, CVE-2025-40048, CVE-2025-40049, CVE-2025-40057, CVE-2025-40064, CVE-2025-40074, CVE-2025-40075, CVE-2025-40078, CVE-2025-40080, CVE-2025-40083, CVE-2025-40104, CVE-2025-40105, CVE-2025-40109, CVE-2025-40123, CVE-			July 2026		41.0

Reference	Description	Severity	Risk	Updated	Impacted versions	Addressed in version
	2025-40125, CVE-2025-40134, CVE-2025-40135, CVE-2025-40139, CVE-2025-40146, CVE-2025-40149, CVE-2025-40153, CVE-2025-40158, CVE-2025-40160, CVE-2025-40167, CVE-2025-40168, CVE-2025-40169, CVE-2025-40170, CVE-2025-40173, CVE-2025-40176, CVE-2025-40178, CVE-2025-40179, CVE-2025-40183, CVE-2025-40190, CVE-2025-40194, CVE-2025-40198, CVE-2025-40200, CVE-2025-40201, CVE-2025-40206, CVE-2025-40215, CVE-2025-40219, CVE-2025-40220, CVE-2025-40248, CVE-2025-40250, CVE-2025-40251, CVE-2025-40254, CVE-2025-40257, CVE-2025-40258, CVE-2025-40259, CVE-2025-40261, CVE-2025-40271, CVE-2025-40272, CVE-2025-40278, CVE-2025-40279, CVE-2025-40292, CVE-2025-40297, CVE-2025-40300, CVE-2025-40304, CVE-2025-40307, CVE-2025-40319, CVE-2025-40322, CVE-2025-40323, CVE-2025-40325, CVE-2025-40341, CVE-2025-40342, CVE-2025-40343, CVE-2025-40350, CVE-2025-40355, CVE-2025-40363, CVE-2025-48038, CVE-2025-48039, CVE-2025-48040, CVE-2025-48041, CVE-2025-50200, CVE-2025-61984, CVE-2025-61985, CVE-2025-62408, CVE-2025-67724, CVE-2025-68160, CVE-2025-68171, CVE-2025-68173, CVE-2025-68178, CVE-2025-68183, CVE-2025-68188, CVE-2025-68191, CVE-2025-68198, CVE-2025-68200, CVE-2025-68206, CVE-2025-68209, CVE-2025-68211, CVE-2025-68214, CVE-2025-68227, CVE-2025-68229, CVE-2025-68231, CVE-2025-68239, CVE-2025-68241, CVE-2025-68245, CVE-2025-68259, CVE-2025-68261, CVE-2025-68264, CVE-2025-68265, CVE-2025-68283, CVE-2025-68284, CVE-2025-68285, CVE-2025-68296, CVE-2025-68321, CVE-2025-68337, CVE-2025-68363, CVE-2025-68366, CVE-2025-68372, CVE-2025-68374, CVE-2025-68378, CVE-2025-68724, CVE-2025-68725, CVE-2025-68736, CVE-2025-68740, CVE-2025-68742, CVE-2025-68744, CVE-2025-68756, CVE-2025-68768, CVE-2025-68775, CVE-2025-68780, CVE-2025-68782, CVE-2025-68785, CVE-2025-68788, CVE-2025-68794, CVE-2025-68795, CVE-2025-68798, CVE-2025-68813, CVE-2025-68814, CVE-2025-68815, CVE-2025-68816, CVE-2025-68823, CVE-2025-69224, CVE-2025-69225, CVE-2025-69226, CVE-2025-69229, CVE-2025-69418, CVE-2025-69419, CVE-2025-69420, CVE-2025-69421, CVE-2025-71066, CVE-2025-71072, CVE-2025-71077, CVE-2025-71084, CVE-2025-71085, CVE-2025-71088, CVE-2025-71089, CVE-2025-71093, CVE-2025-71096, CVE-2025-71097, CVE-2025-71098, CVE-2025-71104, CVE-2025-71113, CVE-2025-71116, CVE-2025-71118, CVE-2025-71125, CVE-2025-71131, CVE-2025-71148, CVE-2025-71152, CVE-2025-71160, CVE-2025-71161, CVE-2025-71202, CVE-2025-71225, CVE-2025-71239, CVE-2025-71285, CVE-2025-71295, CVE-2025-7709, CVE-2026-0665, CVE-2026-0861, CVE-2026-0915, CVE-2026-1207, CVE-2026-1285, CVE-2026-1287, CVE-2026-1312, CVE-2026-1642, CVE-2026-2003, CVE-2026-22695, CVE-2026-22795, CVE-2026-22796, CVE-2026-22801, CVE-2026-22976, CVE-2026-22977, CVE-2026-22984, CVE-2026-22990, CVE-2026-22991, CVE-2026-22992, CVE-2026-22994, CVE-2026-22996, CVE-2026-22999, CVE-2026-23000, CVE-2026-23001, CVE-2026-23004, CVE-2026-23005, CVE-2026-23011, CVE-2026-23025, CVE-2026-23032, CVE-2026-23035, CVE-2026-23047, CVE-2026-23053, CVE-2026-23054, CVE-2026-23060, CVE-2026-23064, CVE-2026-23069, CVE-2026-23074, CVE-2026-23083, CVE-2026-23086, CVE-2026-23087, CVE-2026-23088, CVE-2026-23095, CVE-2026-23097, CVE-2026-23099, CVE-2026-23103, CVE-2026-23105, CVE-2026-23110, CVE-2026-23111, CVE-2026-23112, CVE-2026-23113, CVE-2026-23119, CVE-2026-23120, CVE-2026-23124, CVE-2026-23136, CVE-2026-23138, CVE-2026-23139, CVE-2026-23140, CVE-2026-23154, CVE-2026-23156, CVE-2026-23168, CVE-2026-23171, CVE-2026-23193, CVE-2026-23198, CVE-2026-23204, CVE-2026-23209, CVE-2026-23212, CVE-2026-23216, CVE-2026-23231, CVE-2026-23240, CVE-2026-23243, CVE-2026-23244, CVE-2026-23245, CVE-2026-23247, CVE-2026-23255, CVE-2026-23262, CVE-2026-23268, CVE-2026-23269, CVE-2026-23271, CVE-2026-23272, CVE-2026-23274, CVE-2026-23276, CVE-2026-23277, CVE-2026-23278, CVE-2026-23285, CVE-2026-23292, CVE-2026-23293, CVE-2026-23296, CVE-2026-23300, CVE-2026-23302, CVE-2026-23304, CVE-2026-23310, CVE-2026-23319, CVE-2026-23340, CVE-2026-23343, CVE-2026-23348, CVE-2026-23351, CVE-2026-23352, CVE-2026-23356, CVE-2026-23359, CVE-2026-23368, CVE-2026-23378, CVE-2026-23379, CVE-2026-23381, CVE-2026-23386, CVE-2026-23388, CVE-2026-23391, CVE-2026-23392, CVE-2026-23397, CVE-2026-23398, CVE-2026-23399, CVE-2026-23401, CVE-2026-23403, CVE-2026-23404, CVE-2026-23405, CVE-2026-23406, CVE-2026-23407, CVE-2026-23408, CVE-2026-23409, CVE-2026-23410, CVE-2026-23411, CVE-2026-23412, CVE-2026-23419, CVE-2026-23439, CVE-2026-23441, CVE-2026-23449, CVE-2026-23450, CVE-2026-23452, CVE-2026-23454, CVE-2026-23455, CVE-2026-23456, CVE-2026-23457, CVE-2026-23458, CVE-2026-23472, CVE-2026-23865, CVE-2026-25075, CVE-2026-25646, CVE-2026-25990, CVE-2026-26007, CVE-2026-2673, CVE-2026-3119, CVE-2026-31399, CVE-2026-31414, CVE-2026-31415, CVE-2026-31416, CVE-2026-31418, CVE-2026-31419, CVE-2026-31421, CVE-2026-31422, CVE-2026-31423, CVE-2026-31424, CVE-2026-31425, CVE-2026-31426, CVE-2026-31427, CVE-2026-31428, CVE-2026-31431, CVE-2026-31446, CVE-2026-31447, CVE-2026-31448, CVE-2026-31449, CVE-2026-31450, CVE-2026-31451, CVE-2026-31452, CVE-2026-31469, CVE-					

Reference	Description	Severity	Risk	Updated	Impacted versions	Addressed in version
	2026-31495, CVE-2026-31496, CVE-2026-31503, CVE-2026-31504, CVE-2026-31507, CVE-2026-31515, CVE-2026-31516, CVE-2026-31518, CVE-2026-31521, CVE-2026-31523, CVE-2026-31525, CVE-2026-31527, CVE-2026-31528, CVE-2026-31530, CVE-2026-31546, CVE-2026-31555, CVE-2026-31557, CVE-2026-31674, CVE-2026-31675, CVE-2026-31678, CVE-2026-31679, CVE-2026-31680, CVE-2026-31682, CVE-2026-31738, CVE-2026-31752, CVE-2026-31788, CVE-2026-33416, CVE-2026-33636, CVE-2026-34073, CVE-2026-3497, CVE-2026-3591, CVE-2026-39892, CVE-2026-43010, CVE-2026-43013, CVE-2026-43016, CVE-2026-43025, CVE-2026-43026, CVE-2026-43027, CVE-2026-43028, CVE-2026-43030, CVE-2026-43033, CVE-2026-43035, CVE-2026-43036, CVE-2026-43037, CVE-2026-43038, CVE-2026-43040, CVE-2026-43043, CVE-2026-43048, CVE-2026-43054, CVE-2026-43056, CVE-2026-43060, CVE-2026-43065, CVE-2026-43066, CVE-2026-43068, CVE-2026-43123, CVE-2026-43124, CVE-2026-43128, CVE-2026-43129, CVE-2026-43132, CVE-2026-43133, CVE-2026-43139, CVE-2026-43161, CVE-2026-43163, CVE-2026-43167, CVE-2026-43171, CVE-2026-43186, CVE-2026-43190, CVE-2026-43194, CVE-2026-43197, CVE-2026-43198, CVE-2026-43214, CVE-2026-43216, CVE-2026-43226, CVE-2026-43230, CVE-2026-43233, CVE-2026-43238, CVE-2026-43240, CVE-2026-43244, CVE-2026-43248, CVE-2026-43265, CVE-2026-43266, CVE-2026-43277, CVE-2026-43278, CVE-2026-43281, CVE-2026-43288, CVE-2026-43289, CVE-2026-43303, CVE-2026-43304, CVE-2026-43309, CVE-2026-43313, CVE-2026-43314, CVE-2026-43315, CVE-2026-43328, CVE-2026-43329, CVE-2026-43333, CVE-2026-43339, CVE-2026-43341, CVE-2026-43363, CVE-2026-43366, CVE-2026-43383, CVE-2026-43405, CVE-2026-43406, CVE-2026-43407, CVE-2026-43409, CVE-2026-43428, CVE-2026-43439, CVE-2026-43441, CVE-2026-43445, CVE-2026-43448, CVE-2026-43449, CVE-2026-43450, CVE-2026-43451, CVE-2026-43452, CVE-2026-43453, CVE-2026-43456, CVE-2026-43466, CVE-2026-43468, CVE-2026-43472, CVE-2026-43473, CVE-2026-43475, CVE-2026-43483, CVE-2026-45847, CVE-2026-45848, CVE-2026-45851, CVE-2026-45855, CVE-2026-45856, CVE-2026-45858, CVE-2026-45860, CVE-2026-45862, CVE-2026-45873, CVE-2026-45886, CVE-2026-45890, CVE-2026-45893, CVE-2026-45894, CVE-2026-45895, CVE-2026-45899, CVE-2026-45905, CVE-2026-45912, CVE-2026-45913, CVE-2026-45915, CVE-2026-45917, CVE-2026-45919, CVE-2026-45920, CVE-2026-45932, CVE-2026-45942, CVE-2026-45944, CVE-2026-45948, CVE-2026-45949, CVE-2026-45957, CVE-2026-45962, CVE-2026-45965, CVE-2026-45968, CVE-2026-45970, CVE-2026-45982, CVE-2026-45985, CVE-2026-46253, CVE-2026-46254, CVE-2026-46259, CVE-2026-46266, CVE-2026-46328, CVE-2026-5201					
CVE-2026-50596	Insufficient input validation in the signalling implementation(s) allows a malicious attacker to trigger a software abort resulting in a denial of service. **CVSS3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Mitigation:** None **Resolution:** Upgrade to Pexip Infinity v40.0	High	High	April 2026	35 to 39.1	40.0
CVE-2026-50594	Insufficient input validation in the signalling implementation(s) allows a malicious attacker to trigger a software abort resulting in a denial of service. **CVSS3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Mitigation:** None **Resolution:** Upgrade to Pexip Infinity v40.0	High	High	April 2026	27.0 to 39.1	40.0
CVE-2026-50595	Improper access control can allow exposure of webapp internal information to an untrusted website. **CVSS3.1 base score:** 7.1 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N) **Discussion:** A user must load the Pexip web app via a link on an attacker's website, which could allow an attacker to hijack the web app session. **Mitigation:** None **Resolution:** Upgrade to Pexip Infinity v40.0	High	High	April 2026	30.0 to 39.1	40.0

Reference	Description	Severity	Risk	Updated	Impacted versions	Addressed in version
CVE-2026-23490	pyasn1 is a generic ASN.1 library for Python. Prior to 0.6.2, a Denial-of-Service issue has been found that leads to memory exhaustion from malformed RELATIVE-OID with excessive continuation octets. This vulnerability is fixed in 0.6.2. **CVSS 3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Discussion:** Exploitation on a Pexip Infinity management node would require the presentation of a malicious TLS certificate, either by a malicious intermediary or a client if HTTP client certificate authentication, and could cause a denial of service. Exploitation on a conferencing node would require a malicious intermediary in order to cause a denial of service. **Mitigation:** Access to the management node should be restricted to trusted networks. Administrators should ensure that only trusted HTTP proxies are configured. **Resolution:** Upgrade to Pexip Infinity v40.0	High	High	April 2026	All before 40.0	40.0
Multiple	**Resolved minor issues:** CVE-2024-47619, CVE-2025-10158, CVE-2025-12817, CVE-2025-12818, CVE-2025-13601, CVE-2025-14087, CVE-2025-14512, CVE-2025-15467, CVE-2025-3360, CVE-2025-4373, CVE-2025-50181, CVE-2025-6020, CVE-2025-66293, CVE-2025-66418, CVE-2025-68160, CVE-2025-68973, CVE-2025-69418, CVE-2025-69419, CVE-2025-69420, CVE-2025-69421, CVE-2025-7039, CVE-2025-7345, CVE-2025-9714, CVE-2026-1642, CVE-2026-2003, CVE-2026-21441, CVE-2026-22795, CVE-2026-22796, CVE-2026-22801, CVE-2026-25646, CVE-2026-28387, CVE-2026-28388, CVE-2026-28389, CVE-2026-28390, CVE-2026-31790			April 2026		40.0
CVE-2026-50597	An input validation failure in the Pexip Infinity Administrator interface allows an authenticated remote attacker to execute arbitrary code as an unprivileged user on Pexip Infinity nodes. **CVSS3.1 base score:** 9.1 (AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H) **Discussion:** An attacker must be authenticated to the Pexip Infinity Administrator interface (or API) and have sufficient permissions to access the vulnerable functionality. **Mitigation:** Restrict access to the "May restore system backup" permission to only trusted users. As general good practice, ensure that access to the Pexip Infinity Management Node is restricted to trusted networks using appropriate firewalls. **Resolution:** Upgrade to Pexip Infinity v39.2 **Credit:** This issue was responsibly disclosed by researchers at the NATO Communications and Information Agency (NCIA).	Critical	Critical	July 2026	27.0 to 39.1	39.2
CVE-2025-66443	Insufficient input validation in the signalling implementation(s) allows a malicious attacker to trigger a software abort resulting in a temporary denial of service. **CVSS3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Discussion:** The vulnerability can only be triggered when using Direct Media for WebRTC calls. This functionality is disabled in default configuration and must be configured explicitly by the system administrator. **Mitigation:** Direct Media for WebRTC calls may be disabled on a per-conference basis by navigating to **Services > Virtual Meeting Rooms**, selecting the Virtual Meeting Room to configure and from the **Advanced options** section, changing the **Enable direct media** option to ***Never***. **Resolution:** Upgrade to Pexip Infinity v39.0	High	High	December 2025	35.0 to 38.1	39.0
CVE-2025-66379	Insufficient input validation in the media implementation allows a remote attacker to trigger a software abort resulting in a denial of service. **CVSS3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Discussion:** A crafted media stream may result in a controlled abort during processing. **Mitigation:** None. **Resolution:** Upgrade to Pexip Infinity v39.	High	High	December 2025	All before 39.0	39.0

Reference	Description	Severity	Risk	Updated	Impacted versions	Addressed in version
CVE-2025-66377	Missing authentication on a product-internal API allows an attacker with local access to one node within a Pexip Infinity installation to impact the operation of other nodes within the installation. **CVSS3.1 base score:** 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) **Discussion:** Exploitation requires an attacker to be able to run arbitrary code on a node by either achieving remote code execution via some other vulnerability or having administrative access to the operating system. **Mitigation:** Ensure that only trusted users have credentials for the operating system administration account. Ensure that SSH is disabled across the Pexip Infinity platform and only re-enable it in the rare instances where it is needed. **Resolution:** Upgrade to Pexip Infinity v39. **Credit:** This issue was responsibly disclosed by researchers at the NATO Communications and Information Agency (NCIA).	High	High	December 2025	All before 39.0	39.0
CVE-2025-61920	Authlib is a Python library which builds OAuth and OpenID Connect servers. Prior to version 1.6.5, Authlib's JOSE implementation accepts unbounded JWS/JWT header and signature segments. A remote attacker can craft a token whose base64url-encoded header or signature spans hundreds of megabytes. During verification, Authlib decodes and parses the full input before it is rejected, driving CPU and memory consumption to hostile levels and enabling denial of service. Version 1.6.5 patches the issue. Some temporary workarounds are available. Enforce input size limits before handing tokens to Authlib and/or use application-level throttling to reduce amplification risk. **CVSS 3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Discussion:** Pexip Infinity will use the affected library when validating responses from OIDC identity providers for access to the Management Web Interface or API. **Mitigation:** Administrators should ensure that only trusted Identity Providers are configured for Management Node authentication. **Resolution:** Upgrade to Pexip Infinity v39.	High	High	December 2025	35.0 to 38.1	39.0
CVE-2025-7424	A flaw was found in the libxslt library. The same memory field, psvi, is used for both stylesheet and input data, which can lead to type confusion during XML transformations. This vulnerability allows an attacker to crash the application or corrupt memory. In some cases, it may lead to denial of service or unexpected behavior. **CVSS 3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Discussion:** Pexip Infinity versions before 27 do not expose this component to untrusted input and are thus not directly impacted by this issue (although it is still present in the versions of the component contained in pre-27 Infinity releases). Pexip Infinity versions from 27 up to 38 do process untrusted input using the affected component as part of the Single Sign-On functionality. **Mitigation:** Administrators should ensure that only trusted Identity Providers are configured. **Resolution:** Upgrade to Pexip Infinity v39.	High	High	December 2025	All before 39.0	39.0

Reference	Description	Severity	Risk	Updated	Impacted versions	Addressed in version
CVE-2024-8176	A stack overflow vulnerability exists in the libexpat library due to the way it handles recursive entity expansion in XML documents. When parsing an XML document with deeply nested entity references, libexpat can be forced to recurse indefinitely, exhausting the stack space and causing a crash. This issue could lead to denial of service (DoS) or, in some cases, exploitable memory corruption, depending on the environment and library usage. **CVSS 3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Discussion:** Pexip Infinity uses the Expat XML parser only when configured for integration with external systems (such as CUCM Ad Hoc conferencing). This functionality is disabled in default configuration and must be configured explicitly by the system administrator. **Mitigation:** If integration with CUCM Ad Hoc conferencing is not required, ensure that this functionality is disabled by navigating to **Platform > Global Settings > External System Integration**, clearing the **External system username** and **External system password** fields, and saving the settings. If integration with CUCM Ad Hoc conferencing is required, there is no mitigation available. **Resolution:** Upgrade to Pexip Infinity v39.	High	High	December 2025	All before 39.0	39.0
CVE-2023-52425	libexpat through 2.5.0 allows a denial of service (resource consumption) because many full reparsings are required in the case of a large token for which multiple buffer fills are needed. **CVSS 3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Discussion:** Pexip Infinity uses the Expat XML parser only when configured for integration with external systems (such as CUCM Ad Hoc conferencing). This functionality is disabled in default configuration and must be configured explicitly by the system administrator. **Mitigation:** If integration with CUCM Ad Hoc conferencing is not required, ensure that this functionality is disabled by navigating to **Platform > Global Settings > External System Integration**, clearing the **External system username** and **External system password** fields, and saving the settings. If integration with CUCM Ad Hoc conferencing is required, there is no mitigation available. **Resolution:** Upgrade to Pexip Infinity v39.	High	High	December 2025	All before 39.0	39.0

Reference	Description	Severity	Risk	Updated	Impacted versions	Addressed in version
Multiple	**Resolved minor issues:** CVE-2025-8677, CVE-2025-40778, CVE-2025-40780, CVE-2024-7264, CVE-2025-4748, CVE-2025-46712, CVE-2024-50602, CVE-2025-4802, CVE-2025-8058, CVE-2025-27516, CVE-2025-64505, CVE-2025-64506, CVE-2025-64720, CVE-2025-65018, CVE-2024-24806, CVE-2023-39615, CVE-2023-45322, CVE-2024-25062, CVE-2025-6170, CVE-2025-32414, CVE-2025-49794, CVE-2025-49796, CVE-2023-40403, CVE-2024-27397, CVE-2024-49569, CVE-2024-50017, CVE-2024-50138, CVE-2024-50146, CVE-2024-53209, CVE-2024-53222, CVE-2024-56549, CVE-2024-57977, CVE-2024-58005, CVE-2024-58017, CVE-2024-58078, CVE-2024-58083, CVE-2024-58085, CVE-2024-58088, CVE-2024-58090, CVE-2024-58098, CVE-2024-58100, CVE-2024-58237, CVE-2025-21702, CVE-2025-21706, CVE-2025-21712, CVE-2025-21738, CVE-2025-21745, CVE-2025-21756, CVE-2025-21758, CVE-2025-21759, CVE-2025-21760, CVE-2025-21761, CVE-2025-21762, CVE-2025-21763, CVE-2025-21764, CVE-2025-21765, CVE-2025-21766, CVE-2025-21767, CVE-2025-21779, CVE-2025-21790, CVE-2025-21791, CVE-2025-21814, CVE-2025-21831, CVE-2025-21832, CVE-2025-21836, CVE-2025-21839, CVE-2025-21846, CVE-2025-21853, CVE-2025-21854, CVE-2025-21857, CVE-2025-21858, CVE-2025-21862, CVE-2025-21863, CVE-2025-21864, CVE-2025-21867, CVE-2025-21872, CVE-2025-21875, CVE-2025-21881, CVE-2025-21887, CVE-2025-21889, CVE-2025-21891, CVE-2025-21895, CVE-2025-21898, CVE-2025-21899, CVE-2025-21908, CVE-2025-21913, CVE-2025-21919, CVE-2025-21920, CVE-2025-21926, CVE-2025-21931, CVE-2025-21938, CVE-2025-21951, CVE-2025-21959, CVE-2025-21960, CVE-2025-21966, CVE-2025-21971, CVE-2025-21980, CVE-2025-21991, CVE-2025-21992, CVE-2025-21993, CVE-2025-21997, CVE-2025-21999, CVE-2025-22005, CVE-2025-22021, CVE-2025-22035, CVE-2025-22044, CVE-2025-22045, CVE-2025-22055, CVE-2025-22056, CVE-2025-22057, CVE-2025-22058, CVE-2025-22063, CVE-2025-22064, CVE-2025-22075, CVE-2025-22083, CVE-2025-22086, CVE-2025-22089, CVE-2025-22090, CVE-2025-22126, CVE-2025-23136, CVE-2025-23141, CVE-2025-23142, CVE-2025-23145, CVE-2025-23150, CVE-2025-23163, CVE-2025-37738, CVE-2025-37756, CVE-2025-37772, CVE-2025-37773, CVE-2025-37780, CVE-2025-37785, CVE-2025-37789, CVE-2025-37797, CVE-2025-37798, CVE-2025-37800, CVE-2025-37808, CVE-2025-37820, CVE-2025-37823, CVE-2025-37836, CVE-2025-37839, CVE-2025-37857, CVE-2025-37859, CVE-2025-37867, CVE-2025-37878, CVE-2025-37884, CVE-2025-37885, CVE-2025-37890, CVE-2025-37911, CVE-2025-37913, CVE-2025-37914, CVE-2025-37915, CVE-2025-37921, CVE-2025-37923, CVE-2025-37928, CVE-2025-37932, CVE-2025-37936, CVE-2025-37938, CVE-2025-37940, CVE-2025-37949, CVE-2025-37957, CVE-2025-37958, CVE-2025-37959, CVE-2025-37960, CVE-2025-37961, CVE-2025-37980, CVE-2025-37988, CVE-2025-37992, CVE-2025-37995, CVE-2025-37997, CVE-2025-37998, CVE-2025-38000, CVE-2025-38001, CVE-2025-38008, CVE-2025-38018, CVE-2025-38020, CVE-2025-38035, CVE-2025-38037, CVE-2025-38039, CVE-2025-38040, CVE-2025-38048, CVE-2025-38058, CVE-2025-38061, CVE-2025-38062, CVE-2025-38063, CVE-2025-38066, CVE-2025-38067, CVE-2025-38068, CVE-2025-38071, CVE-2025-38072, CVE-2025-38074, CVE-2025-38075, CVE-2025-38078, CVE-2025-38079, CVE-2025-38083, CVE-2025-38084, CVE-2025-38085, CVE-2025-38087, CVE-2025-38095, CVE-2025-38097, CVE-2025-38100, CVE-2025-38102, CVE-2025-38103, CVE-2025-38107, CVE-2025-38108, CVE-2025-38110, CVE-2025-38111, CVE-2025-38112, CVE-2025-38113, CVE-2025-38115, CVE-2025-38122, CVE-2025-38146, CVE-2025-38147, CVE-2025-38148, CVE-2025-38149, CVE-2025-38161, CVE-2025-38165, CVE-2025-38166, CVE-2025-38177, CVE-2025-38181, CVE-2025-38182, CVE-2025-38192, CVE-2025-38193, CVE-2025-38198, CVE-2025-38202, CVE-2025-38211, CVE-2025-38212, CVE-2025-38214, CVE-2025-38215, CVE-2025-38220, CVE-2025-38222, CVE-2025-38236, CVE-2025-38246, CVE-2025-38255, CVE-2025-38263, CVE-2025-38280, CVE-2025-38282, CVE-2025-38285, CVE-2025-38305, CVE-2025-38310, CVE-2025-38312, CVE-2025-38324, CVE-2025-38326, CVE-2025-38334, CVE-2025-38337, CVE-2025-38342, CVE-2025-38344, CVE-2025-38345, CVE-2025-38346, CVE-2025-38349, CVE-2025-38352, CVE-2025-38364, CVE-2025-38375, CVE-2025-38386, CVE-2025-38387, CVE-2025-38396, CVE-2025-38399, CVE-2025-38403, CVE-2025-38415, CVE-2025-38424, CVE-2025-38439, CVE-2025-38443, CVE-2025-38444, CVE-2025-38445, CVE-2025-38455, CVE-2025-38457, CVE-2025-38461, CVE-2025-38462, CVE-2025-38463, CVE-2025-38465, CVE-2025-38466, CVE-2025-38468, CVE-2025-38470, CVE-2025-38471, CVE-2025-38472, CVE-2025-38477, CVE-2025-38494, CVE-2025-38495, CVE-2025-38496, CVE-2025-38498, CVE-2025-38637, CVE-2025-39989, CVE-2025-40364, CVE-2025-53859, CVE-2025-9230, CVE-2025-9232, CVE-2023-31484, CVE-2025-40909, CVE-2025-59420, CVE-2025-62706, CVE-2025-57833, CVE-2025-64459, CVE-2024-5569, CVE-2025-47273, CVE-2025-6965, CVE-2025-29087, CVE-2025-29088, CVE-2025-62291, CVE-2025-32462			December 2025		39.0

Reference	Description	Severity	Risk	Updated	Impacted versions	Addressed in version
CVE-2025-66378	Insufficient access control in the RTMP implementation allows a malicious attacker to disconnect RTMP streams traversing a Proxy Node. **CVSS3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Discussion:** RTMP is used to stream conference media to external recording implementations. **Mitigation:** This issue may be mitigated by disabling support for RTMP via **Platform > Global Settings > Connectivity**. However, if RTMP streaming is required, no mitigation is available. **Resolution:** Upgrade to Pexip Infinity v38.2.	High	High	July 2026	38.0, 38.1	38.2
CVE-2025-59683	Improper access control in the Secure Scheduler for Exchange service, when used with Office 365 Legacy Exchange Tokens, allows a remote attacker to read potentially sensitive data and excessively consume resources, leading to a denial of service. **CVSS3.1 base score:** 8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H) **Mitigation:** Customers using Office 365 and are running Pexip Infinity Version 37.1 or newer should ensure that all of their Secure Scheduler for Exchange integrations are using an "Add-in authentication token type" of "SSO Token" or "NAA (Nested App Authentication) Token". **Resolution:** Upgrade to Pexip Infinity v38.1	High	High	October 2025	15.0 - 38.0	38.1
CVE-2025-48704	Insufficient input validation in the signalling implementation(s) allows a malicious attacker to trigger a software abort resulting in a denial of service. **CVSS3.1 base score:** 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **Mitigation:** None **Resolution:** Upgrade to Pexip Infinity v38	High	High	July 2025	35.0 - 37.2	38.0
CVE-2025-24855	numbers.c in libxslt before 1.1.43 has a use-after-free because, in nested XPath evaluations, an XPath context node can be modified but never restored. This is related to xsltNumberFormatGetValue, xsltEvalXPathPredicate, xsltEvalXPathStringNs, and xsltComputeSortResultInternal. **CVSS 3.1 base score:** 8.7 (AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:H) **Discussion:** Infinity versions before 27 do not expose this component to untrusted input and are thus not directly impacted by this issue (although it is still present in the versions of the component contained in pre-27 Infinity releases). Infinity versions from 27 up to 38 do process untrusted input using the affected component as part of the Single Sign-On functionality. **Mitigation:** Administrators should ensure that only trusted Identity Providers are configured. **Resolution:** Upgrade to Pexip Infinity v38.	High	High	July 2025	All before 38.0	38.0
CVE-2024-55549	xsltGetInheritedNsList in libxslt before 1.1.43 has a use-after-free issue related to exclusion of result prefixes. **CVSS3.1 base score:** 8.7 (AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:H) **Discussion:** Infinity versions before 27 do not expose this component to untrusted input and are thus not directly impacted by this issue (although it is still present in the versions of the component contained in pre-27 Infinity releases). Infinity versions from 27 up to 38 do process untrusted input using the affected component as part of the Single Sign-On functionality. **Mitigation:** Administrators should ensure that only trusted Identity Providers are configured. **Resolution:** Upgrade to Pexip Infinity v38.	High	High	July 2025	All before 38.0	38.0
Multiple	**Resolved minor issues:** CVE-2011-10007, CVE-2022-49043, CVE-2023-29383, CVE-2023-4039, CVE-2023-4641, CVE-2023-48795, CVE-2023-51385, CVE-2023-51767, CVE-2024-56171, CVE-2024-56406, CVE-2024-7347, CVE-2025-0938, CVE-2025-1390, CVE-2025-22247, CVE-2025-22866, CVE-2025-22870, CVE-2025-24928, CVE-2025-26699, CVE-2025-27113, CVE-2025-31115, CVE-2025-32415, CVE-2025-32728, CVE-2025-32873, CVE-2025-4207, CVE-2025-4598, CVE-2025-46836, CVE-2025-48432, CVE-2025-6199			July 2025		38.0

Legacy Connect apps

From **1 November 2025**, the legacy Connect desktop apps and Connect mobile apps are no longer supported for general purpose usage. The Connect desktop app for Windows remains supported for use in Citrix environments only.

For security bulletins relating to the Connect apps, see our v39 documentation site.

VMR self-service portal

Each bulletin addresses a number of vulnerabilities in the software used by the VMR self-service portal. The bulletins include an assessment of the issues, the impact on the VMR portal, and resolution details.

Bulletin	Description	Risk	Updated	Impacted versions	Addressed in version
CVE-2023-40236	The Pexip VMR self-service portal before v3 uses the same SSH host keys across different customers' installations, which allows man-in-the-middle attackers to spoof fake instances by leveraging these keys. **CVSS 3.1 base score:** 7.5 (AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H) **Mitigation:** Manually remove and regenerate the SSH host keys on each VMR Portal instance. **Resolution:** Upgrade to VMR portal v3.	High	October 2023	All prior to version 3	3

Enhanced Room Management

Each bulletin addresses a number of vulnerabilities in the software used by ERM. The bulletins include an assessment of the issues, the impact on the VMR portal, and resolution details.

Bulletin	Description	Risk	Updated	Impacted versions	Addressed in version
CVE-2024-6387	A race condition was found in OpenSSH's server. If a client does not authenticate within 120 seconds then sshd's SIGALRM handler is called asynchronously and calls various functions that are not async-signal-safe. An unauthenticated remote attacker could exploit this vulnerability to execute arbitrary code with root privileges. **CVSS3.1 base score:** 8.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) **Mitigation:** The mitigation for older versions (prior to v2.0.1) is to disable the **Proxy service** in the ERM Installer and redeploy, however we recommend upgrading to v2.0.1 as soon as practicable. **Resolution:** Install v2.0.1 security upgrade 2024-07-09.	High	July 2024	All prior to version 2.0.1	2.0.1 security upgrade 2024-07-09

AIMS

Bulletin	Description	Risk	Updated	Impacted versions	Addressed in version
	Resolved minor issues: CVE-2011-10007, CVE-2022-49043, CVE-2023-0180, CVE-2023-0183, CVE-2023-0184, CVE-2023-0185, CVE-2023-0187, CVE-2023-0188, CVE-2023-0189, CVE-2023-0190, CVE-2023-0191, CVE-2023-0194, CVE-2023-0195, CVE-2023-0198, CVE-2023-0199, CVE-2023-4039, CVE-2023-4641, CVE-2023-25515, CVE-2023-25516, CVE-2023-28370, CVE-2023-29383, CVE-2023-31022, CVE-2023-31124, CVE-2023-31147, CVE-2023-31484, CVE-2023-39615, CVE-2023-40403, CVE-2023-45322, CVE-2023-48795, CVE-2023-49081, CVE-2023-49082, CVE-2023-51385, CVE-2023-51767, CVE-2023-52425, CVE-2023-52920, CVE-2024-0074, CVE-2024-0075, CVE-2024-0078, CVE-2024-0090, CVE-2024-0092, CVE-2024-0126, CVE-2024-0131, CVE-2024-0147, CVE-2024-0149, CVE-2024-0150, CVE-2024-5569, CVE-2024-7347, CVE-2024-8096, CVE-2024-8176, CVE-2024-8244, CVE-2024-12086, CVE-2024-12747, CVE-2024-13176, CVE-2024-25062, CVE-2024-25629, CVE-2024-26686, CVE-2024-27011, CVE-2024-27017, CVE-2024-27397, CVE-2024-28182, CVE-2024-34459, CVE-2024-36478, CVE-2024-43835, CVE-2024-45231, CVE-2024-45336, CVE-2024-45341, CVE-2024-46678, CVE-2024-46679, CVE-2024-46695, CVE-2024-46711, CVE-2024-46713, CVE-2024-46713, CVE-2024-46717, CVE-2024-46721, CVE-2024-46735, CVE-2024-46737, CVE-2024-46738, CVE-2024-46738, CVE-2024-46739, CVE-2024-46744, CVE-2024-46744, CVE-2024-46746, CVE-2024-46746, CVE-2024-46750, CVE-2024-46762, CVE-2024-46763, CVE-2024-46777, CVE-2024-46782, CVE-2024-46782, CVE-2024-46783, CVE-2024-46784, CVE-2024-46787, CVE-2024-46794, CVE-2024-46826, CVE-2024-46829, CVE-2024-46830, CVE-2024-46830, CVE-2024-46848, CVE-2024-46855, CVE-2024-46858, CVE-2024-46858, CVE-2024-47660, CVE-2024-47668, CVE-2024-47674, CVE-2024-47678, CVE-2024-47679, CVE-2024-47682, CVE-2024-47682, CVE-2024-47684, CVE-2024-47685, CVE-2024-47685, CVE-2024-47693, CVE-2024-47701, CVE-2024-47701, CVE-2024-47705, CVE-2024-47706, CVE-2024-47707, CVE-2024-47710, CVE-2024-47727, CVE-2024-47727, CVE-2024-47728, CVE-2024-47734, CVE-2024-47739, CVE-2024-47742, CVE-2024-47742, CVE-2024-47743, CVE-2024-47745, CVE-2024-47745, CVE-2024-47748, CVE-2024-47748, CVE-2024-49568, CVE-2024-49569, CVE-2024-49850, CVE-2024-49851, CVE-2024-49855, CVE-2024-49855, CVE-2024-49856, CVE-2024-49858, CVE-2024-49860, CVE-2024-49860, CVE-2024-49861, CVE-2024-49861, CVE-2024-49863, CVE-2024-49870, CVE-2024-49878, CVE-2024-49881, CVE-2024-49882, CVE-2024-49882, CVE-2024-49883, CVE-2024-49883, CVE-2024-49884, CVE-2024-49884, CVE-2024-49889, CVE-2024-49889, CVE-2024-49925, CVE-2024-49926, CVE-2024-49927, CVE-2024-49933, CVE-2024-49934, CVE-2024-49935, CVE-2024-49936, CVE-2024-49948, CVE-2024-49949, CVE-2024-49952, CVE-2024-49954, CVE-2024-49959, CVE-2024-49960, CVE-2024-49960, CVE-2024-49973, CVE-2024-49975, CVE-2024-49978, CVE-2024-49983, CVE-2024-49983, CVE-2024-49994, CVE-2024-50000, CVE-2024-50001, CVE-2024-50002, CVE-2024-50006, CVE-2024-50009, CVE-2024-50010, CVE-2024-50012, CVE-2024-50013, CVE-2024-50014, CVE-2024-50015, CVE-2024-50017, CVE-2024-50019, CVE-2024-50022, CVE-2024-50024, CVE-2024-50036, CVE-2024-50036, CVE-2024-50038, CVE-2024-50039, CVE-2024-50045, CVE-2024-50046, CVE-2024-50048, CVE-2024-50055, CVE-2024-50055, CVE-2024-50058, CVE-2024-50060, CVE-2024-50063, CVE-2024-50063, CVE-2024-50067, CVE-2024-50067, CVE-2024-50082, CVE-2024-50083, CVE-2024-50083, CVE-2024-50093, CVE-2024-50095, CVE-2024-50110, CVE-2024-50115, CVE-2024-50115, CVE-2024-50126, CVE-2024-50126, CVE-2024-50127, CVE-2024-50127, CVE-2024-50131, CVE-2024-50131, CVE-2024-50135, CVE-2024-50138, CVE-2024-50141, CVE-2024-50142, CVE-2024-50143, CVE-2024-50143, CVE-2024-50146, CVE-2024-50147, CVE-2024-50153, CVE-2024-50154, CVE-2024-50154, CVE-2024-50162, CVE-2024-50163, CVE-2024-50164, CVE-2024-50164, CVE-2024-50182, CVE-2024-50184, CVE-2024-50185, CVE-2024-50189, CVE-2024-50191, CVE-2024-50195, CVE-2024-50199, CVE-2024-50200, CVE-2024-50211, CVE-2024-50226, CVE-2024-50226, CVE-2024-50250, CVE-2024-50250, CVE-2024-50251, CVE-2024-50256, CVE-2024-50257, CVE-2024-50257, CVE-2024-50258, CVE-2024-50261, CVE-2024-50261, CVE-2024-50262, CVE-2024-50262, CVE-2024-50264, CVE-2024-50264, CVE-2024-50271, CVE-2024-50272, CVE-2024-50278, CVE-2024-50278, CVE-2024-50279, CVE-2024-50279, CVE-2024-50280, CVE-2024-50280, CVE-2024-50301, CVE-2024-50301, CVE-2024-50302, CVE-2024-50304, CVE-2024-50602, CVE-2024-53042, CVE-2024-53052, CVE-2024-53057, CVE-2024-53057, CVE-2024-53079, CVE-2024-53082, CVE-2024-53082, CVE-2024-53085, CVE-2024-53091, CVE-2024-53093, CVE-2024-53099, CVE-2024-53099, CVE-2024-53105, CVE-2024-53124, CVE-2024-53125, CVE-2024-53128, CVE-2024-53141, CVE-2024-53141, CVE-2024-53142, CVE-2024-53142, CVE-2024-53164, CVE-2024-53166, CVE-2024-53166, CVE-2024-53170, CVE-2024-53170, CVE-2024-53175, CVE-2024-53194, CVE-2024-53194, CVE-2024-53198, CVE-2024-53209, CVE-2024-53214, CVE-2024-53214, CVE-2024-53222, CVE-2024-53224, CVE-2024-53233, CVE-2024-53240, CVE-2024-53241, CVE-2024-53869, CVE-2024-54683, CVE-2024-55549, CVE-2024-56171, CVE-2024-56406, CVE-2024-56549, CVE-2024-56566, CVE-2024-56569, CVE-2024-56570, CVE-2024-56570, CVE-2024-56583, CVE-2024-56584, CVE-2024-56587, CVE-2024-56592, CVE-2024-56600, CVE-2024-56600, CVE-2024-56601, CVE-2024-56601, CVE-2024-56606, CVE-2024-56606, CVE-2024-56611, CVE-2024-56614, CVE-2024-56614, CVE-2024-56615, CVE-2024-56615, CVE-2024-56631, CVE-2024-56631, CVE-2024-56633, CVE-2024-56633, CVE-2024-56636, CVE-2024-56637, CVE-		October 2025		2.0

Bulletin	Description	Risk	Updated	Impacted versions	Addressed in version
	2024-56640, CVE-2024-56640, CVE-2024-56641, CVE-2024-56644, CVE-2024-56658, CVE-2024-56658, CVE-2024-56662, CVE-2024-56664, CVE-2024-56664, CVE-2024-56672, CVE-2024-56672, CVE-2024-56675, CVE-2024-56675, CVE-2024-56693, CVE-2024-56693, CVE-2024-56703, CVE-2024-56709, CVE-2024-56718, CVE-2024-56720, CVE-2024-56739, CVE-2024-56745, CVE-2024-56751, CVE-2024-56756, CVE-2024-56763, CVE-2024-56770, CVE-2024-56780, CVE-2024-56786, CVE-2024-56786, CVE-2024-57843, CVE-2024-57882, CVE-2024-57883, CVE-2024-57884, CVE-2024-57888, CVE-2024-57890, CVE-2024-57900, CVE-2024-57900, CVE-2024-57903, CVE-2024-57917, CVE-2024-57917, CVE-2024-57924, CVE-2024-57929, CVE-2024-57929, CVE-2024-57931, CVE-2024-57940, CVE-2024-57977, CVE-2024-58005, CVE-2024-58017, CVE-2024-58078, CVE-2024-58083, CVE-2024-58085, CVE-2024-58088, CVE-2024-58090, CVE-2024-58098, CVE-2024-58100, CVE-2024-58237, CVE-2025-0938, CVE-2025-1390, CVE-2025-4207, CVE-2025-4598, CVE-2025-4673, CVE-2025-4802, CVE-2025-6021, CVE-2025-6170, CVE-2025-6199, CVE-2025-6965, CVE-2025-7424, CVE-2025-7425, CVE-2025-8058, CVE-2025-8713, CVE-2025-9230, CVE-2025-9232, CVE-2025-21648, CVE-2025-21653, CVE-2025-21664, CVE-2025-21665, CVE-2025-21666, CVE-2025-21667, CVE-2025-21669, CVE-2025-21680, CVE-2025-21681, CVE-2025-21683, CVE-2025-21700, CVE-2025-21701, CVE-2025-21702, CVE-2025-21706, CVE-2025-21712, CVE-2025-21738, CVE-2025-21745, CVE-2025-21756, CVE-2025-21758, CVE-2025-21759, CVE-2025-21760, CVE-2025-21761, CVE-2025-21762, CVE-2025-21763, CVE-2025-21764, CVE-2025-21765, CVE-2025-21766, CVE-2025-21767, CVE-2025-21779, CVE-2025-21790, CVE-2025-21791, CVE-2025-21814, CVE-2025-21831, CVE-2025-21836, CVE-2025-21839, CVE-2025-21846, CVE-2025-21853, CVE-2025-21854, CVE-2025-21857, CVE-2025-21858, CVE-2025-21862, CVE-2025-21863, CVE-2025-21864, CVE-2025-21867, CVE-2025-21872, CVE-2025-21875, CVE-2025-21881, CVE-2025-21887, CVE-2025-21889, CVE-2025-21891, CVE-2025-21895, CVE-2025-21898, CVE-2025-21899, CVE-2025-21908, CVE-2025-21913, CVE-2025-21919, CVE-2025-21920, CVE-2025-21926, CVE-2025-21931, CVE-2025-21938, CVE-2025-21951, CVE-2025-21959, CVE-2025-21960, CVE-2025-21966, CVE-2025-21971, CVE-2025-21980, CVE-2025-21991, CVE-2025-21992, CVE-2025-21993, CVE-2025-21997, CVE-2025-21999, CVE-2025-22005, CVE-2025-22021, CVE-2025-22035, CVE-2025-22044, CVE-2025-22045, CVE-2025-22055, CVE-2025-22056, CVE-2025-22057, CVE-2025-22058, CVE-2025-22063, CVE-2025-22064, CVE-2025-22075, CVE-2025-22083, CVE-2025-22086, CVE-2025-22089, CVE-2025-22090, CVE-2025-22126, CVE-2025-22247, CVE-2025-22866, CVE-2025-22870, CVE-2025-22871, CVE-2025-23136, CVE-2025-23141, CVE-2025-23142, CVE-2025-23145, CVE-2025-23150, CVE-2025-23163, CVE-2025-23244, CVE-2025-24855, CVE-2025-24928, CVE-2025-27113, CVE-2025-31115, CVE-2025-32414, CVE-2025-32415, CVE-2025-32462, CVE-2025-32728, CVE-2025-32873, CVE-2025-37738, CVE-2025-37756, CVE-2025-37772, CVE-2025-37773, CVE-2025-37780, CVE-2025-37785, CVE-2025-37789, CVE-2025-37797, CVE-2025-37798, CVE-2025-37800, CVE-2025-37808, CVE-2025-37820, CVE-2025-37823, CVE-2025-37836, CVE-2025-37839, CVE-2025-37857, CVE-2025-37859, CVE-2025-37867, CVE-2025-37878, CVE-2025-37884, CVE-2025-37885, CVE-2025-37890, CVE-2025-37911, CVE-2025-37913, CVE-2025-37914, CVE-2025-37915, CVE-2025-37921, CVE-2025-37923, CVE-2025-37928, CVE-2025-37932, CVE-2025-37936, CVE-2025-37938, CVE-2025-37940, CVE-2025-37949, CVE-2025-37957, CVE-2025-37958, CVE-2025-37959, CVE-2025-37960, CVE-2025-37961, CVE-2025-37980, CVE-2025-37988, CVE-2025-37992, CVE-2025-37997, CVE-2025-37998, CVE-2025-38000, CVE-2025-38008, CVE-2025-38018, CVE-2025-38020, CVE-2025-38035, CVE-2025-38037, CVE-2025-38039, CVE-2025-38040, CVE-2025-38048, CVE-2025-38058, CVE-2025-38061, CVE-2025-38062, CVE-2025-38063, CVE-2025-38066, CVE-2025-38067, CVE-2025-38068, CVE-2025-38071, CVE-2025-38072, CVE-2025-38074, CVE-2025-38075, CVE-2025-38078, CVE-2025-38079, CVE-2025-38083, CVE-2025-38084, CVE-2025-38085, CVE-2025-38087, CVE-2025-38095, CVE-2025-38097, CVE-2025-38100, CVE-2025-38102, CVE-2025-38103, CVE-2025-38107, CVE-2025-38108, CVE-2025-38110, CVE-2025-38111, CVE-2025-38112, CVE-2025-38113, CVE-2025-38115, CVE-2025-38122, CVE-2025-38146, CVE-2025-38147, CVE-2025-38148, CVE-2025-38149, CVE-2025-38161, CVE-2025-38165, CVE-2025-38166, CVE-2025-38177, CVE-2025-38181, CVE-2025-38182, CVE-2025-38192, CVE-2025-38193, CVE-2025-38198, CVE-2025-38202, CVE-2025-38211, CVE-2025-38212, CVE-2025-38214, CVE-2025-38215, CVE-2025-38220, CVE-2025-38222, CVE-2025-38236, CVE-2025-38246, CVE-2025-38255, CVE-2025-38263, CVE-2025-38280, CVE-2025-38282, CVE-2025-38285, CVE-2025-38305, CVE-2025-38310, CVE-2025-38312, CVE-2025-38324, CVE-2025-38326, CVE-2025-38334, CVE-2025-38337, CVE-2025-38342, CVE-2025-38344, CVE-2025-38345, CVE-2025-38346, CVE-2025-38349, CVE-2025-38352, CVE-2025-38364, CVE-2025-38375, CVE-2025-38386, CVE-2025-38387, CVE-2025-38396, CVE-2025-38399, CVE-2025-38403, CVE-2025-38415, CVE-2025-38424, CVE-2025-38439, CVE-2025-38443, CVE-2025-38444, CVE-2025-38445, CVE-2025-38455, CVE-2025-38457, CVE-2025-38461, CVE-2025-38462, CVE-2025-38463, CVE-2025-38465, CVE-2025-38466, CVE-2025-38468, CVE-2025-38470, CVE-2025-38471, CVE-2025-38477, CVE-2025-38494, CVE-2025-38495, CVE-2025-38496, CVE-2025-38498, CVE-2025-38637, CVE-2025-39989, CVE-2025-40364, CVE-2025-40909, CVE-2025-46712, CVE-2025-46836, CVE-2025-47906, CVE-2025-48432, CVE-2025-49794, CVE-2025-49796, CVE-2025-53859				

© 2026 Pexip AS v42. By using Pexip Software and Services you accept our Terms and Privacy Statement. Learn more about Pexip.