Vulnerability Report (High & Critical Only)

Software: 7-Zip 24.09 (x64) (24.09)
CVE ID: CVE-2016-2335 | Severity: HIGH
The CInArchive::ReadFileItem method in Archive/Udf/UdfIn.cpp in 7zip 9.20 and 15.05 beta and p7zip allows remote attackers to cause a denial of service (out-of-bounds read) or execute arbitrary code via the PartitionRef field in the Long Allocation Descriptor in a UDF file.

Software: 7-Zip 24.09 (x64) (24.09)
CVE ID: CVE-2016-4300 | Severity: HIGH
Integer overflow in the read_SubStreamsInfo function in archive_read_support_format_7zip.c in libarchive before 3.2.1 allows remote attackers to execute arbitrary code via a 7zip file with a large number of substreams, which triggers a heap-based buffer overflow.

Software: 7-Zip 24.09 (x64) (24.09)
CVE ID: CVE-2016-2334 | Severity: HIGH
Heap-based buffer overflow in the NArchive::NHfs::CHandler::ExtractZlibFile method in 7zip before 16.00 and p7zip allows remote attackers to execute arbitrary code via a crafted HFS+ image.

Software: 7-Zip 24.09 (x64) (24.09)
CVE ID: CVE-2016-8689 | Severity: HIGH
The read_Header function in archive_read_support_format_7zip.c in libarchive 3.2.1 allows remote attackers to cause a denial of service (out-of-bounds read) via multiple EmptyStream attributes in a header in a 7zip archive.

Software: Git (2.43.0)
CVE ID: CVE-2012-2055 | Severity: HIGH
GitHub Enterprise before 20120304 does not properly restrict the use of a hash to provide values for a model's attributes, which allows remote attackers to set the public_key[user_id] value via a modified URL for the public-key update form, related to a "mass assignment" vulnerability.

Software: Git (2.43.0)
CVE ID: CVE-2016-2315 | Severity: CRITICAL
revision.c in git before 2.7.4 uses an incorrect integer data type, which allows remote attackers to execute arbitrary code via a (1) long filename or (2) many nested trees, leading to a heap-based buffer overflow.

Software: Git (2.43.0)
CVE ID: CVE-2016-2324 | Severity: CRITICAL
Integer overflow in Git before 2.7.4 allows remote attackers to execute arbitrary code via a (1) long filename or (2) many nested trees, which triggers a heap-based buffer overflow.

Software: Git (2.43.0)
CVE ID: CVE-2015-7545 | Severity: CRITICAL
The (1) git-remote-ext and (2) unspecified other remote helper programs in Git before 2.3.10, 2.4.x before 2.4.10, 2.5.x before 2.5.4, and 2.6.x before 2.6.1 do not properly restrict the allowed protocols, which might allow remote attackers to execute arbitrary code via a URL in a (a) .gitmodules file or (b) unknown other sources in a submodule.

Software: Git (2.43.0)
CVE ID: CVE-2016-3068 | Severity: HIGH
Mercurial before 3.7.3 allows remote attackers to execute arbitrary code via a crafted git ext:: URL when cloning a subrepository.

Software: Git (2.43.0)
CVE ID: CVE-2016-3069 | Severity: HIGH
Mercurial before 3.7.3 allows remote attackers to execute arbitrary code via a crafted name when converting a Git repository.

Software: Git (2.43.0)
CVE ID: CVE-2016-3105 | Severity: HIGH
The convert extension in Mercurial before 3.8 might allow context-dependent attackers to execute arbitrary code via a crafted git repository name.

Software: Git (2.43.0)
CVE ID: CVE-2015-8968 | Severity: HIGH
git-fastclone before 1.0.1 permits arbitrary shell command execution from .gitmodules. If an attacker can instruct a user to run a recursive clone from a repository they control, they can get a client to run an arbitrary shell command. Alternately, if an attacker can MITM an unencrypted git clone, they could exploit this. The ext command will be run if the repository is recursively cloned or if submodules are updated. This attack works when cloning both local and remote repositories.

Software: Git (2.43.0)
CVE ID: CVE-2015-8969 | Severity: CRITICAL
git-fastclone before 1.0.5 passes user modifiable strings directly to a shell command. An attacker can execute malicious commands by modifying the strings that are passed as arguments to "cd " and "git clone " commands in the library.

Software: Git (2.43.0)
CVE ID: CVE-2016-9274 | Severity: HIGH
Untrusted search path vulnerability in Git 1.x for Windows allows local users to gain privileges via a Trojan horse git.exe file in the current working directory. NOTE: 2.x is unaffected.

Software: Git (2.43.0)
CVE ID: CVE-2016-10075 | Severity: HIGH
The tqdm._version module in tqdm versions 4.4.1 and 4.10 allows local users to execute arbitrary code via a crafted repo with a malicious git log in the current working directory.

Software: Git (2.43.0)
CVE ID: CVE-2016-7793 | Severity: HIGH
sociomantic-tsunami git-hub before 0.10.3 allows remote attackers to execute arbitrary code via a crafted repository URL.

Software: Git (2.43.0)
CVE ID: CVE-2016-7794 | Severity: CRITICAL
sociomantic-tsunami git-hub before 0.10.3 allows remote attackers to execute arbitrary code via a crafted repository name.

Software: Git (2.43.0)
CVE ID: CVE-2016-4340 | Severity: HIGH
The impersonate feature in Gitlab 8.7.0, 8.6.0 through 8.6.7, 8.5.0 through 8.5.11, 8.4.0 through 8.4.9, 8.3.0 through 8.3.8, and 8.2.0 through 8.2.4 allows remote authenticated users to "log in" as any other user via unspecified vectors.

Software: Notepad++ (64-bit x64) (8.2.1)
CVE ID: CVE-2017-8803 | Severity: HIGH
Notepad++ 7.3.3 (32-bit) with Hex Editor Plugin v0.9.5 might allow user-assisted attackers to execute code via a crafted file, because of a "Data from Faulting Address controls Code Flow" issue. One threat model is a victim who obtains an untrusted crafted file from a remote location and issues several user-defined commands.

Software: Notepad++ (64-bit x64) (8.2.1)
CVE ID: CVE-2019-16294 | Severity: HIGH
SciLexer.dll in Scintilla in Notepad++ (x64) before 7.7 allows remote code execution or denial of service via Unicode characters in a crafted .ml file.

Software: Notepad++ (64-bit x64) (8.2.1)
CVE ID: CVE-2022-32168 | Severity: HIGH
Notepad++ versions 8.4.1 and before are vulnerable to DLL hijacking where an attacker can replace the vulnerable dll (UxTheme.dll) with his own dll and run arbitrary code in the context of Notepad++.

Software: Notepad++ (64-bit x64) (8.2.1)
CVE ID: CVE-2023-40031 | Severity: HIGH
Notepad++ is a free and open-source source code editor. Versions 8.5.6 and prior are vulnerable to heap buffer write overflow in `Utf8_16_Read::convert`. This issue may lead to arbitrary code execution. As of time of publication, no known patches are available in existing versions of Notepad++.

Software: Notepad++ (64-bit x64) (8.2.1)
CVE ID: CVE-2023-47452 | Severity: HIGH
An Untrusted search path vulnerability in notepad++ 6.5 allows local users to gain escalated privileges through the msimg32.dll file in the current working directory.

Software: XAMPP (8.2.12-0)
CVE ID: CVE-2018-17933 | Severity: HIGH
VGo Robot (Versions 3.0.3.52164 and 3.0.3.53662. Prior versions may also be affected) connected to the VGo XAMPP. User accounts may be able to execute commands that are outside the scope of their privileges and within the scope of an admin account. If an attacker has access to VGo XAMPP Client credentials, they may be able to execute admin commands on the connected robot.

Software: XAMPP (8.2.12-0)
CVE ID: CVE-2019-8923 | Severity: CRITICAL
XAMPP through 5.6.8 and previous allows SQL injection via the cds-fpdf.php jahr parameter. NOTE: This product is discontinued.

Software: XAMPP (8.2.12-0)
CVE ID: CVE-2020-11107 | Severity: HIGH
An issue was discovered in XAMPP before 7.2.29, 7.3.x before 7.3.16 , and 7.4.x before 7.4.4 on Windows. An unprivileged user can change a .exe configuration in xampp-contol.ini for all users (including admins) to enable arbitrary command execution.

Software: XAMPP (8.2.12-0)
CVE ID: CVE-2022-29376 | Severity: HIGH
Xampp for Windows v8.1.4 and below was discovered to contain insecure permissions for its install directory, allowing attackers to execute arbitrary code via overwriting binaries located in the directory.

Software: XAMPP (8.2.12-0)
CVE ID: CVE-2024-0338 | Severity: HIGH
A buffer overflow vulnerability has been found in XAMPP affecting version 8.2.4 and earlier. An attacker could execute arbitrary code through a long file debug argument that controls the Structured Exception Handler (SEH).

Software: XAMPP (8.2.12-0)
CVE ID: CVE-2024-5055 | Severity: HIGH
Uncontrolled resource consumption vulnerability in XAMPP Windows, versions 7.3.2 and earlier. This vulnerability exists when XAMPP attempts to process many incomplete HTTP requests, resulting in resource consumption and system crashes.

Software: Python 3.12.1 pip Bootstrap (64-bit) (3.12.1150.0)
CVE ID: CVE-2005-3302 | Severity: HIGH
Eval injection vulnerability in bvh_import.py in Blender 2.36 allows attackers to execute arbitrary Python code via a hierarchy element in a .bvh file, which is supplied to an eval function call.

Software: Python 3.12.1 pip Bootstrap (64-bit) (3.12.1150.0)
CVE ID: CVE-2007-4559 | Severity: CRITICAL
Directory traversal vulnerability in the (1) extract and (2) extractall functions in the tarfile module in Python allows user-assisted remote attackers to overwrite arbitrary files via a .. (dot dot) sequence in filenames in a TAR archive, a related issue to CVE-2001-1267.

Software: Universal CRT Tools x64 (10.1.22621.3233)
CVE ID: CVE-2002-1706 | Severity: HIGH
Cisco IOS software 11.3 through 12.2 running on Cisco uBR7200 and uBR7100 series Universal Broadband Routers allows remote attackers to modify Data Over Cable Service Interface Specification (DOCSIS) settings via a DOCSIS file without a Message Integrity Check (MIC) signature, which is approved by the router.

Software: Universal CRT Tools x64 (10.1.22621.3233)
CVE ID: CVE-2004-0389 | Severity: HIGH
RealNetworks Helix Universal Server 9.0.1 and 9.0.2 allows remote attackers to cause a denial of service (crash) via malformed requests that trigger a null dereference, as demonstrated using (1) GET_PARAMETER or (2) DESCRIBE requests.

Software: Python 3.12.1 Executables (64-bit) (3.12.1150.0)
CVE ID: CVE-2005-3302 | Severity: HIGH
Eval injection vulnerability in bvh_import.py in Blender 2.36 allows attackers to execute arbitrary Python code via a hierarchy element in a .bvh file, which is supplied to an eval function call.

Software: Python 3.12.1 Executables (64-bit) (3.12.1150.0)
CVE ID: CVE-2007-4559 | Severity: CRITICAL
Directory traversal vulnerability in the (1) extract and (2) extractall functions in the tarfile module in Python allows user-assisted remote attackers to overwrite arbitrary files via a .. (dot dot) sequence in filenames in a TAR archive, a related issue to CVE-2001-1267.

Software: Python 3.12.1 Standard Library (64-bit) (3.12.1150.0)
CVE ID: CVE-2005-3302 | Severity: HIGH
Eval injection vulnerability in bvh_import.py in Blender 2.36 allows attackers to execute arbitrary Python code via a hierarchy element in a .bvh file, which is supplied to an eval function call.

Software: Python 3.12.1 Standard Library (64-bit) (3.12.1150.0)
CVE ID: CVE-2007-4559 | Severity: CRITICAL
Directory traversal vulnerability in the (1) extract and (2) extractall functions in the tarfile module in Python allows user-assisted remote attackers to overwrite arbitrary files via a .. (dot dot) sequence in filenames in a TAR archive, a related issue to CVE-2001-1267.

Software: PuTTY release 0.78 (64-bit) (0.78.0.0)
CVE ID: CVE-2016-2563 | Severity: CRITICAL
Stack-based buffer overflow in the SCP command-line utility in PuTTY before 0.67 and KiTTY 0.66.6.3 and earlier allows remote servers to cause a denial of service (stack memory corruption) or execute arbitrary code via a crafted SCP-SINK file-size response to an SCP download request.

Software: PuTTY release 0.78 (64-bit) (0.78.0.0)
CVE ID: CVE-2016-6167 | Severity: HIGH
Multiple untrusted search path vulnerabilities in Putty beta 0.67 allow local users to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse (1) UxTheme.dll or (2) ntmarta.dll file in the current working directory.

Software: PuTTY release 0.78 (64-bit) (0.78.0.0)
CVE ID: CVE-2017-6542 | Severity: CRITICAL
The ssh_agent_channel_data function in PuTTY before 0.68 allows remote attackers to have unspecified impact via a large length value in an agent protocol message and leveraging the ability to connect to the Unix-domain socket representing the forwarded agent connection, which trigger a buffer overflow.

Software: PuTTY release 0.78 (64-bit) (0.78.0.0)
CVE ID: CVE-2019-9894 | Severity: HIGH
A remotely triggerable memory overwrite in RSA key exchange in PuTTY before 0.71 can occur before host key verification.

Software: PuTTY release 0.78 (64-bit) (0.78.0.0)
CVE ID: CVE-2019-9895 | Severity: CRITICAL
In PuTTY versions before 0.71 on Unix, a remotely triggerable buffer overflow exists in any kind of server-to-client forwarding.

Software: PuTTY release 0.78 (64-bit) (0.78.0.0)
CVE ID: CVE-2019-9896 | Severity: HIGH
In PuTTY versions before 0.71 on Windows, local attackers could hijack the application by putting a malicious help file in the same directory as the executable.

Software: PuTTY release 0.78 (64-bit) (0.78.0.0)
CVE ID: CVE-2019-9897 | Severity: HIGH
Multiple denial-of-service attacks that can be triggered by writing to the terminal exist in PuTTY versions before 0.71.

Software: PuTTY release 0.78 (64-bit) (0.78.0.0)
CVE ID: CVE-2019-9898 | Severity: CRITICAL
Potential recycling of random numbers used in cryptography exists within PuTTY before 0.71.

Software: PuTTY release 0.78 (64-bit) (0.78.0.0)
CVE ID: CVE-2019-17067 | Severity: CRITICAL
PuTTY before 0.73 on Windows improperly opens port-forwarding listening sockets, which allows attackers to listen on the same port to steal an incoming connection.

Software: PuTTY release 0.78 (64-bit) (0.78.0.0)
CVE ID: CVE-2019-17068 | Severity: HIGH
PuTTY before 0.73 mishandles the "bracketed paste mode" protection mechanism, which may allow a session to be affected by malicious clipboard content.

Software: PuTTY release 0.78 (64-bit) (0.78.0.0)
CVE ID: CVE-2019-17069 | Severity: HIGH
PuTTY before 0.73 might allow remote SSH-1 servers to cause a denial of service by accessing freed memory locations via an SSH1_MSG_DISCONNECT message.

Software: PuTTY release 0.78 (64-bit) (0.78.0.0)
CVE ID: CVE-2021-33500 | Severity: HIGH
PuTTY before 0.75 on Windows allows remote servers to cause a denial of service (Windows GUI hang) by telling the PuTTY window to change its title repeatedly at high speed, which results in many SetWindowTextA or SetWindowTextW calls. NOTE: the same attack methodology may affect some OS-level GUIs on Linux or other platforms for similar reasons.

Software: PuTTY release 0.78 (64-bit) (0.78.0.0)
CVE ID: CVE-2021-36367 | Severity: HIGH
PuTTY through 0.75 proceeds with establishing an SSH session even if it has never sent a substantive authentication response. This makes it easier for an attacker-controlled SSH server to present a later spoofed authentication prompt (that the attacker can use to capture credential data, and use that data for purposes that are undesired by the client user).

Software: Bonjour (3.1.0.1)
CVE ID: CVE-2016-1364 | Severity: HIGH
Cisco Wireless LAN Controller (WLC) Software 7.4 before 7.4.130.0(MD) and 7.5, 7.6, and 8.0 before 8.0.110.0(ED) allows remote attackers to cause a denial of service (device reload) via crafted Bonjour traffic, aka Bug ID CSCur66908.

Software: Python 3.12.1 Documentation (64-bit) (3.12.1150.0)
CVE ID: CVE-2005-3302 | Severity: HIGH
Eval injection vulnerability in bvh_import.py in Blender 2.36 allows attackers to execute arbitrary Python code via a hierarchy element in a .bvh file, which is supplied to an eval function call.

Software: Python 3.12.1 Documentation (64-bit) (3.12.1150.0)
CVE ID: CVE-2007-4559 | Severity: CRITICAL
Directory traversal vulnerability in the (1) extract and (2) extractall functions in the tarfile module in Python allows user-assisted remote attackers to overwrite arbitrary files via a .. (dot dot) sequence in filenames in a TAR archive, a related issue to CVE-2001-1267.

Software: Python 3.12.1 Development Libraries (64-bit) (3.12.1150.0)
CVE ID: CVE-2005-3302 | Severity: HIGH
Eval injection vulnerability in bvh_import.py in Blender 2.36 allows attackers to execute arbitrary Python code via a hierarchy element in a .bvh file, which is supplied to an eval function call.

Software: Python 3.12.1 Development Libraries (64-bit) (3.12.1150.0)
CVE ID: CVE-2007-4559 | Severity: CRITICAL
Directory traversal vulnerability in the (1) extract and (2) extractall functions in the tarfile module in Python allows user-assisted remote attackers to overwrite arbitrary files via a .. (dot dot) sequence in filenames in a TAR archive, a related issue to CVE-2001-1267.

Software: Python 3.12.1 Tcl/Tk Support (64-bit) (3.12.1150.0)
CVE ID: CVE-2005-3302 | Severity: HIGH
Eval injection vulnerability in bvh_import.py in Blender 2.36 allows attackers to execute arbitrary Python code via a hierarchy element in a .bvh file, which is supplied to an eval function call.

Software: Python 3.12.1 Tcl/Tk Support (64-bit) (3.12.1150.0)
CVE ID: CVE-2007-4559 | Severity: CRITICAL
Directory traversal vulnerability in the (1) extract and (2) extractall functions in the tarfile module in Python allows user-assisted remote attackers to overwrite arbitrary files via a .. (dot dot) sequence in filenames in a TAR archive, a related issue to CVE-2001-1267.

Software: Python 3.12.1 Add to Path (64-bit) (3.12.1150.0)
CVE ID: CVE-2005-3302 | Severity: HIGH
Eval injection vulnerability in bvh_import.py in Blender 2.36 allows attackers to execute arbitrary Python code via a hierarchy element in a .bvh file, which is supplied to an eval function call.

Software: Python 3.12.1 Add to Path (64-bit) (3.12.1150.0)
CVE ID: CVE-2007-4559 | Severity: CRITICAL
Directory traversal vulnerability in the (1) extract and (2) extractall functions in the tarfile module in Python allows user-assisted remote attackers to overwrite arbitrary files via a .. (dot dot) sequence in filenames in a TAR archive, a related issue to CVE-2001-1267.

Software: Python 3.12.1 Core Interpreter (64-bit) (3.12.1150.0)
CVE ID: CVE-2005-3302 | Severity: HIGH
Eval injection vulnerability in bvh_import.py in Blender 2.36 allows attackers to execute arbitrary Python code via a hierarchy element in a .bvh file, which is supplied to an eval function call.

Software: Python 3.12.1 Core Interpreter (64-bit) (3.12.1150.0)
CVE ID: CVE-2007-4559 | Severity: CRITICAL
Directory traversal vulnerability in the (1) extract and (2) extractall functions in the tarfile module in Python allows user-assisted remote attackers to overwrite arbitrary files via a .. (dot dot) sequence in filenames in a TAR archive, a related issue to CVE-2001-1267.

Software: Update for x64-based Windows Systems (KB5001716) (8.94.0.0)
CVE ID: CVE-2000-1218 | Severity: CRITICAL
The default configuration for the domain name resolver for Microsoft Windows 98, NT 4.0, 2000, and XP sets the QueryIpMatching parameter to 0, which causes Windows to accept DNS updates from hosts that it did not query, which allows remote attackers to poison the DNS cache.

Software: Update for x64-based Windows Systems (KB5001716) (8.94.0.0)
CVE ID: CVE-2000-0944 | Severity: CRITICAL
CGI Script Center News Update 1.1 does not properly validate the original news administration password during a password change operation, which allows remote attackers to modify the password without knowing the original password.

Software: Update for x64-based Windows Systems (KB5001716) (8.94.0.0)
CVE ID: CVE-2001-0497 | Severity: HIGH
dnskeygen in BIND 8.2.4 and earlier, and dnssec-keygen in BIND 9.1.2 and earlier, set insecure permissions for a HMAC-MD5 shared secret key file used for DNS Transactional Signatures (TSIG), which allows attackers to obtain the keys and perform dynamic DNS updates.

Software: Update for x64-based Windows Systems (KB5001716) (8.94.0.0)
CVE ID: CVE-2001-1125 | Severity: CRITICAL
Symantec LiveUpdate before 1.6 does not use cryptography to ensure the integrity of download files, which allows remote attackers to execute arbitrary code via DNS spoofing of the update.symantec.com site.

Software: Python 3.12.1 Test Suite (64-bit) (3.12.1150.0)
CVE ID: CVE-2005-3302 | Severity: HIGH
Eval injection vulnerability in bvh_import.py in Blender 2.36 allows attackers to execute arbitrary Python code via a hierarchy element in a .bvh file, which is supplied to an eval function call.

Software: Python 3.12.1 Test Suite (64-bit) (3.12.1150.0)
CVE ID: CVE-2007-4559 | Severity: CRITICAL
Directory traversal vulnerability in the (1) extract and (2) extractall functions in the tarfile module in Python allows user-assisted remote attackers to overwrite arbitrary files via a .. (dot dot) sequence in filenames in a TAR archive, a related issue to CVE-2001-1267.

Software: Dynamic Application Loader Host Interface Service (1.0.0.0)
CVE ID: CVE-2001-0497 | Severity: HIGH
dnskeygen in BIND 8.2.4 and earlier, and dnssec-keygen in BIND 9.1.2 and earlier, set insecure permissions for a HMAC-MD5 shared secret key file used for DNS Transactional Signatures (TSIG), which allows attackers to obtain the keys and perform dynamic DNS updates.
