What is a Downgrade Attack? | CrowdStrike

Archived: 2026-04-06 01:54:41 UTC

Maintaining good cybersecurity means protecting against multiple kinds of attack. One of these attack types is called a “downgrade attack.” This form of cryptographic attack is also called a “version rollback attack” or a “bidding-down attack.” In a downgrade attack, an attacker forces the target system to switch to a low-quality, less secure mode of operation.

Downgrade attacks can take a variety of forms. We’ll talk here about the most common forms of downgrade attack: the form these attacks can take, what functions they serve and how they work. Thankfully, downgrade attacks are well known and well documented at this point, so you don’t have to break new ground in order to protect your company against them.

What Are Downgrade Attacks?

The world of cybersecurity is vast and varied, but not all cyberattacks employ the latest techniques and exploits. **Downgrade attacks** take advantage of a system’s backward compatibility to force it into less secure modes of operation. Because they can use encrypted or unencrypted connections, systems such as STARTTLS that employ opportunistic encryption are at the greatest risk from downgrade attacks.

In an HTTPS downgrade attack, visitors to your website may be forced to use HTTP connections instead of HTTPS. A downgrade attack can be a small part of a larger malicious operation, as was the case in 2015 when the Logjam attack was developed. A TLS downgrade attack such as Logjam allows man-in-the-middle attackers to downgrade transport layer security (TLS) connections to 512-bit cryptography, letting the attackers read all data passed over this insecure connection. We’ll explain more about Logjam and other types of downgrade attack in the next section.

In general, any system that employs any form of backward compatibility can be susceptible to a downgrade attack. The balance between maximum utility and maximum security is a difficult one to strike: however tempting it may be to enforce your visitors to keep their systems updated, you want people to be able to access your server using older technology.

Types of Downgrade Attacks

Downgrade attacks can take many forms, but they all have a few elements in common. Most of them are man-in-the-middle attacks (also called MITM attacks). In these attacks, malicious actors place themselves between your users and your network.

A few of the best-known downgrade attacks include:

- **POODLE**: The Padding Oracle on Downgraded Legacy Encryption attack inserts itself into communications sessions, forcing certain web browsers to downgrade to Secure Sockets Layer (SSL) 3.0

when TLS is unavailable.

- **FREAK**: Similar to POODLE, the Factoring RSA Export Keys vulnerability forces clients to use weak encryption, gaining access to data traffic that can then be easily decrypted.
- **Logjam**: A Logjam exploit combines vulnerabilities in RSA with a flaw in the TLS protocol. In Logjam downgrade attacks, the message a server sends for key exchange is replaced with a weaker variant.
- **BEAST**: The Browser Exploit Against SSL/TLS protocol uses cipher block chaining mode encryption, combining a MITM attack with a chosen boundary attack and record splitting. This attack can let attackers decrypt HTTPS client-server sessions and even get authentication tokens in older SSL and TLS products.
- **SLOTH**: Also known as Security Losses from Obsolete and Truncated Transcript Hashes, SLOTH attacks allow a man in the middle to force web browsers to rely on old, weak hashing algorithms.

Risks of Downgrade Attacks

Because the spectrum of downgrade attacks is so wide, it can be difficult to quantify their risks. A downgrade attack that uses a lower simple mail transfer protocol version may cause a vastly different level of damage than one that employs a cryptographic attack. In all cases, however, being vulnerable to a downgrade attack also makes your server more vulnerable to a larger series of cyberattacks.

Think of a downgrade attack as a lockpick: while using one on someone else's system is a crime in its own right, its real danger is what an attacker can do with the access they gain. A downgrade attack can leave all your company's data vulnerable, from your user account credentials and payment information to your personal medical data.

With every potential downgrade attack, consider what information is at the greatest risk. A system that forces a downgrade from Kerberos to NTLM, for instance, is vulnerable to many types of brute force and "pass the hash" attacks. Ask yourself what information hackers may gain access to and lock down the avenues of access to this information.

The older the protocols are that you support, the more effective a downgrade attack can be. In an ideal world, nobody would have to support older versions of TLS, for instance. In practice, however, many networks still have to support these versions. Firms can minimize their level of risk by only allowing backward compatibility in specific situations and by enforcing compliance with specific, modern versions of TLS whenever possible.

How to Protect Against Downgrade Attacks

The most secure accounts and servers are the ones that account for downgrade attacks and proactively protect against them. Prevention is worth more than a cure in this case: keep your TLS configuration as up to date as possible and remove unnecessary backward compatibility. If you do have to support older versions of the protocol, you should always implement TLS_FALLBACK_SCSV as a protective measure.

TLS 1.3 includes proactive downgrade protection mechanisms, ensuring that all participants in a "handshake" are using the most upgraded security protocols even if there is a man in the middle monitoring the transmissions. More best practices for preventing downgrade attacks include the following:

- Do not use language that assures your users of a secure connection unless you require that connection to be on a validated HTTPS session.
- Prioritize using web protocols such as HTTP/2 that use only TLS, without providing visitors the ability to downgrade.
- Above all, serve as much traffic as you can over TLS, even when that traffic isn't sensitive. Implementing TLS as your default method of connection prevents the vast majority of downgrade attacks from taking hold, no matter what else you do.

Once you've implemented these best practices, you can focus on building infrastructure that detects and mitigates attempted downgrade attacks as they happen. Keep the version of TLS you use up to date, even when upgrading means putting in a lot of time and effort. Once you do that, you should easily be able to track less secure traffic on your servers. In turn, this enables you to spot traffic changes and detect men in the middle before they can do extensive damage to your servers, your reputation and your company as a whole.

CrowdStrike Cyberattack Prevention Solution

Downgrade attacks may seem simple on their own. However, wily attackers can use them as a tool in a much larger arsenal, making protecting against these attacks a critical element of any company's cybersecurity operations. If you aren't sure where to begin when it comes to preventing a downgrade attack, consult with a team of cybersecurity experts to discover what works well and what elements of your operations you can improve.

CrowdStrike's expert team proactively hunts, investigates and advises on activity in your environment to ensure cyber threats are not missed. To learn more about the CrowdStrike Falcon® platform, contact our organization to schedule a demo or enroll in a trial.
